

Risikoorientierte Systematik zur Bewertung von Rückfallebenenkonzepten des Bahnbetriebs

Von der
Fakultät Architektur, Bauingenieurwesen und Umweltwissenschaften
der Technischen Universität Carolo-Wilhelmina
zu Braunschweig

zur Erlangung des Grades eines
Doktor-Ingenieurs (Dr.-Ing.)
genehmigte

Dissertation

von
Po-Chi Huang
geboren am 12. April 1983
aus Taichung City

Eingereicht am: 06. Dezember 2019

Disputation am: 26. Februar 2020

Berichtersteller/in: Prof. Dr.-Ing. Jörn Pachl
Prof. Dr.-Ing. Birgit Milius

2020

Kurzfassung

Durch die zunehmende Anwendung von Informationstechnik (IT) im Eisenbahnwesen bekommt auch die Frage nach ausreichender und gewährleisteter IT-Security einen neuen und wichtigen Stellenwert. Die Bedrohung der IT-Security und ihre Auswirkung auf den Bahnbetrieb sind mittlerweile durch die gesetzlichen Anforderungen und die IT-Security-Vorfälle der Vergangenheit den Fachleuten sehr bewusst. Unabhängig von den getroffenen Vorkehrungen muss davon ausgegangen werden, dass nicht jeder Angriff tatsächlich festgestellt und abgewendet werden kann. Dies bedeutet, dass der Bahnbetrieb nach einem vermuteten oder tatsächlichen IT-Angriff teilweise oder ggf. komplett in der Rückfallebene betrieben werden muss.

Das Rückfallebenenkonzept des Bahnbetriebs hat die Bestrebung, den Bahnbetrieb trotz des Einflusses der vorgegebenen Unregelmäßigkeiten stets mit einer annehmbaren kollektiven Betriebsqualität aus Sicherheit, Leistungsniveau und Verfügbarkeit zu erzielen. Das heutige Rückfallebenenkonzept des Bahnbetriebs ist darauf ausgelegt, die bisher anzunehmenden betrieblichen Einschränkungen, in der Regel Safety-Ereignisse und deren Folgen, zu beherrschen. Das sind zumeist kleinräumige und kurzzeitig andauernde Störungen. Wird der Kreis der möglichen Ursachen nun um den IT-Angriff erweitert, dann ist zu erwarten, dass der zukünftige Bahnbetrieb nicht nur häufig in der Rückfallebene durchgeführt werden muss, sondern auch häufiger mit Mehrfachausfällen von Betriebsfunktionen sowie großräumigen und lang andauernden Störungsszenarien konfrontiert sein wird.

Um die Qualitäten des künftigen Störungsbetriebs systematisch bewerten zu können, wurde im Rahmen dieser Arbeit, gefördert mit dem Grant der Karl-Vossloh-Stiftung (2017-2019), eine risikoorientierte Systematik zur Bewertung von Rückfallebenenkonzepten des Bahnbetriebs entwickelt. Diese Bewertungssystematik ermöglicht die zusammenhängende Berücksichtigung des Störungsszenarios, der systemtechnischen Auslegung, des dynamischen IT-Umfelds, der Charakteristiken des IT-Angriffs sowie die Auslastung der Menschen. Die Anwendung der Bewertungssystematik verfolgt im Wesentlichen das Ziel, die Anwender bei der Gestaltung und der Entscheidungsfindung von Rückfallebenenkonzepten in einer aktuellen dynamischen Betriebslage durch eine schnelle, aber aussagekräftige Risikoschätzung zu unterstützen.

Abstract

Due to the increased use of information technology (IT) in railway systems, the need for sufficient and ensured IT security for railway operation has gained significance in recent years. The railway experts are currently very conscious of the threat of IT security and its impact on railway operations due to the legal requirements and the incidents that happened in the past. Regardless the precautions it must be assumed that not every attack can be detected and averted. As a result, the railway operation might need to be operated partly or completely in degraded mode in case of an assumed or real IT attack.

The purpose of railway operational concepts in degraded mode is to achieve an acceptable operational quality while considering the criterion safety, performance and availability despite the impact of known irregularities during operation. Today's operational concepts in degraded mode are generally designed to deal with irregularities in operation resulting non-intentional safety events and their related impacts. Those irregularities are mostly disturbances restricted to a small area with a very short duration. However, if we consider possible irregularities resulting IT attacks in future operation, the railway operation might need to be operated in the degraded mode not only more frequently but also in longer durations, due to facing complex and large-scale disturbances.

In order to evaluate the operational quality of the railway operation in degraded mode systematically, a risk-oriented systematic has been developed within this thesis, which was funded by the Karl-Vossloh-Stiftung (2017-2019). This systematic enables a joint consideration of operational concepts, system design, dynamic IT environment, characteristic of IT attacks and workload of the staff in the degraded operation. The use of this approach aims to provide a simplified risk evaluation process with a meaningful basis for decision making when choosing the operational concept in degraded mode.

Inhaltsverzeichnis

1	Einleitung.....	1
2	IT-Security und Bahnbetrieb.....	7
2.1	Safety oder Security?	7
2.2	Die Charakteristik des IT-Security-Angriffs	10
2.2.1	Wahrscheinlichkeit	11
2.2.2	Offenbarung.....	12
2.2.3	Ausmaß.....	13
2.2.4	Priorität	15
2.2.5	Dauer	15
2.2.6	Zusammenfassung.....	16
2.3	Bahnbetrieb und dessen Rückfallebenenkonzept.....	18
2.3.1	Bestandteile des Bahnsystems und dessen Aufgaben.....	18
2.3.2	Qualitätsmerkmale des Bahnbetriebs	21
2.3.3	Die rechtliche Forderung auf die Rückfallebene des Bahnbetriebs	23
2.3.4	Der Übergangsprozess zwischen dem Normalbetrieb und der Rückfallebene	25
2.3.5	Die Tätigkeitsfelder des Rückfallebenenkonzepts im Bahnbetrieb	27
2.3.5.1	Tätigkeitsfeld Betriebsleitung.....	27
2.3.5.2	Tätigkeitsfeld Betriebsführung.....	28
2.3.5.3	Tätigkeitsfeld Ereignisbehandlung	29
2.3.5.4	Wechselwirkung zwischen den Tätigkeitsfeldern.....	29
2.3.6	Das Strukturprinzip des Rückfallebenenkonzepts.....	30
2.3.6.1	Strukturblock Ausführungsvariante	31
2.3.6.2	Strukturblock Qualitätsziel.....	33
2.3.6.3	Strukturblock Übergangsregel.....	33
3	Die Bewertungssystematik und deren Anwendungsprinzipien.....	35
3.1	Anforderungen an die Bewertungssystematik	35
3.1.1	Die Herausforderung des künftigen Störungsbetriebs	35
3.1.2	Berücksichtigung der Charakteristiken des IT-Angriffs	37
3.1.3	Berücksichtigung der menschlichen Auslastung	38
3.1.4	Berücksichtigung der Qualitätsmerkmale des Bahnbetriebs.....	40
3.2	Das Anwendungsziel und die Anwendergruppe	43
3.3	Das Betriebsrisiko im Bahnbetrieb	46

3.3.1	Der Kontext des Betriebsrisikos.....	46
3.3.2	Der Risikogrenzwert des Betriebsrisikos.....	49
3.3.3	Mit der Risiko-Budgetierung zur proaktiven Steuerung des Betriebsrisikos.....	58
3.4	Die risikoorientierte Bewertungssystematik	68
3.4.1	Das Risikomodell und die Übersicht der Systematik.....	68
3.4.2	Die Struktur der Bewertungssystematik	74
3.4.2.1	Strukturteil - Betriebsszenario	74
3.4.2.2	Strukturteil - Funktionsmodell.....	79
3.4.2.3	Strukturteil - Versagenspotenzial.....	84
3.4.2.4	Strukturteil - Anzahl der Versagen	98
3.4.2.5	Strukturteil - IT-Manipulationspotenzial	100
3.4.2.6	Strukturteil - Reduktionsfaktor.....	106
3.4.2.7	Strukturteil - Schadensausmaß.....	113
3.4.3	Die Ergebnisse der Bewertung	121
3.4.3.1	Sicherheit des Bahnbetriebs	121
3.4.3.2	Leistungsniveau des Bahnbetriebs.....	123
3.4.3.3	Verfügbarkeit des Bahnbetriebs	124
4	Die Bewertungssystematik in der Anwendung	127
4.1	Phase 1: Die Grundparameter festlegen.....	128
4.2	Phase 2: Das Störungsszenario bestimmen	130
4.3	Phase 3: Qualität der Konzeptvariante ermitteln	132
4.4	Phase 4: Rückfallebenenkonzept gestalten.....	143
4.4.1	Die Basisvariante.....	143
4.4.1.1	Basisvariante-1.....	144
4.4.1.2	Basisvariante-2.....	145
4.4.1.3	Basisvariante-3.....	146
4.4.1.4	Basisvariante-4.....	147
4.4.1.5	Basisvariante-5.....	149
4.4.1.6	Basisvariante-6.....	150
4.4.1.7	Basisvariante-7	151
4.4.1.8	Basisvariante-8.....	152
4.4.1.9	Basisvariante-9.....	153
4.4.1.10	Basisvariante-10.....	154
4.4.1.11	Zusammenfassung	155
4.4.2	Das kombinierte Rückfallebenenkonzept	157

4.4.2.1	Kombiniertes Rückfallebenenkonzept A	158
4.4.2.2	Kombiniertes Rückfallebenenkonzept B	160
4.4.2.3	Kombiniertes Rückfallebenenkonzept C	161
4.4.2.4	Kombiniertes Rückfallebenenkonzept D	163
4.4.2.5	Zusammenfassung	164
5	Diskussion	165
5.1	Maßnahmen zur Erhöhung der Betriebsqualität.....	165
5.1.1	Maßnahmen zur Erhöhung der Sicherheit.....	165
5.1.2	Maßnahmen zur Erhöhung des Leistungsniveaus.....	167
5.1.3	Maßnahmen zu Erhöhung der technischen Verfügbarkeit.....	168
5.2	Konzept einer temporären Räumungsprüfstelle.....	170
5.2.1	Bereich einer temporären Räumungsprüfstelle.....	170
5.2.2	Räumungsprüfung auf einer temporären Räumungsprüfstelle	172
5.2.3	Betriebsablauf zwischen temporären Räumungsprüfstellen	173
6	Fazit und Ausblick.....	176
	Abkürzungsverzeichnis	179
	Literaturverzeichnis	180
	Anhang A: Mittlere Beförderungsgeschwindigkeit	187
	Anhang B: Unfallklasse nach VDE V 0831-103 [85]	188
	Anhang C: Zuordnung von Unfallvariablen zu der Opferzahl	189
	Anhang D: Fahrzeitsimulation zwischen Zmst A und Zmst B	191
	Anhang E: Tagesganglinie Streckenstandard M160	194
	Anhang F: Ablaufplan des Rückfallebenenkonzepts A.....	195
	Anhang G: Ablaufplan des Rückfallebenenkonzepts B	197
	Anhang H: Ablaufplan des Rückfallebenenkonzepts C	199
	Anhang I: Ablaufplan des Rückfallebenenkonzepts D	201

Abbildungsverzeichnis

Abbildung 1: Verbreitete Anwendung von IT im Eisenbahnsystem.....	1
Abbildung 2: Von Ransomware WannaCry betroffenen Fahrgastanzeige im Mai 2017 [8].....	2
Abbildung 3: Strukturaufbau der Arbeit	5
Abbildung 4: Eine taxonomische Übersicht von Safety, Security und deren Folge auf Bahnbetrieb.....	9
Abbildung 5: Bestandteile eines modernen Eisenbahnsystems	19
Abbildung 6: Elementare Aufgaben der Bahn.....	21
Abbildung 7: Ausschlaggebende Qualitätsmerkmale des Bahnsystems	23
Abbildung 8: Bestehender Systemprozessablauf im Bahnbetrieb [1].....	25
Abbildung 9: Tätigkeitsfelder des Rückfallebenenkonzepts	27
Abbildung 10: Schematische Darstellung des Strukturprinzips von Rückfallebenenkonzepten.....	30
Abbildung 11: Wirkungskette eines IT-Angriffs auf die Rückfallebene im Bahnbetrieb	36
Abbildung 12: Wechselwirkung der Beförderungsgeschwindigkeit und Betriebsdichte nach [72].....	41
Abbildung 13: Organisationsstruktur des DB Netz AG während der Störung nach [82, 83]	45
Abbildung 14: Aufbau der Risk Score Matrix in VDE V 0831-103 [85].....	50
Abbildung 15: Maßnahmen zur Einschränkung der Flexibilität der Risiko-Budgetierung.....	67
Abbildung 16: Risikomodell der vorliegenden Bewertungssystematik nach [22].....	68
Abbildung 17: Strukturübersicht der risikoorientierten Bewertungssystematik	69
Abbildung 18: Kombination aus Teilfunktionen des Funktionsmodells im Fehlerbaum	79
Abbildung 19: Unterteilung des Versagenspotenzials nach dessen maßgeblicher Akteur	84
Abbildung 20: Konzept des Versagenspotenzials eines Funktionsmodells von Akteur Technik	85
Abbildung 21: Konzept der auslastungsbedingte Versagenswahrscheinlichkeit des Fdl.....	86
Abbildung 22: Konzept eines Handlungsablaufs	87
Abbildung 23: Konzept eines Funktionsablaufs.....	90
Abbildung 24: Konzept des Versagenspotenzials eines Funktionsmodells von Akteur Fdl	94
Abbildung 25: Konzept des Versagenspotenzials eines Funktionsmodells von Akteur Tf	94
Abbildung 26: Zusammenführung von technischem und menschlichem Versagen im Funktionsmodell.....	98
Abbildung 27: Variablen zum Bestimmen des Schadensausmaßes	113
Abbildung 28: Ablauf der Bewertung.....	127
Abbildung 29: Schematische Darstellung des Gesamtbereichs der Betrachtung	128
Abbildung 30: Schematische Darstellung von dem Bereich der betrieblichen Störung	130
Abbildung 31: Die Verkehrszeiten und Tagesganglinie von Streckenstandard M 160 nach [95]	157
Abbildung 32: Schematische Darstellung von drei temporären Räumungsprüfstellen A, B und C	171
Abbildung 33: Betriebsablauf zwischen den temporären Räumungsprüfstellen	174

Abbildungen, die keine Quellenangabe besitzen, wurden vom Autor persönlich erstellt.

Tabellenverzeichnis

Tabelle 1: Vergleich von Safety-Ereignis und IT-Security-Angriff anhand beispielhafter Kriterien	16
Tabelle 2: Charakteristik des IT-Angriffs und die Anforderungen an die Systematik	38
Tabelle 3: Einflussfaktoren auf die menschliche Auslastung und die Anforderungen an die Systematik	40
Tabelle 4: Qualitätsmerkmale des Bahnbetriebs und die daraus resultierenden Anforderungen	42
Tabelle 5: Vergleich von technischem Risiko und Betriebsrisiko.	49
Tabelle 6: Unfallklasse der RSM und deren Anzahl Opfer nach der Umrechnung	51
Tabelle 7: Vereinfachte Risikoschätzung des Betriebsrisikos bei einem technisch gesicherten Regelbetrieb für Schienenverkehr in Deutschland	54
Tabelle 8: Anzahl Opfer Eisenbahnunfall in Deutschland von 2006 bis 2017 nach [92, 93]	55
Tabelle 9: Anpassung des Risikogrenzwerts nach Risiko und Anteil des Streckenstandards.	57
Tabelle 10: Prioritäten von Störungen bei der DB Netz AG nach [105, 106]	61
Tabelle 11: Mittlere Störbestehenszeiten im Bereich der DB Netz AG im Zeitraum von 2010 bis 2018	61
Tabelle 12: Unterschied zwischen dem technischen und betrieblichen Störungsbereich	77
Tabelle 13: Betriebsfunktionen des Funktionsmodelles und deren Funktionsziele	83
Tabelle 14: Punkteskala Faktor 1 – Dauer der Handlung	88
Tabelle 15: Punkteskala Faktor 2 – Umfang der Handlung	89
Tabelle 16: Punkteskala Faktor 3 – Intensität der Handlung	92
Tabelle 17: Zuordnungsbeispiel einer auslastungsbedingten Versagenswahrscheinlichkeit des Fdl	93
Tabelle 18: Beispiel Tätigkeit des Tf und dessen Auslastung im Regelbetrieb	96
Tabelle 19: Beispiel Tätigkeit des Tf und dessen Auslastung im Störungsbetrieb	96
Tabelle 20: Zuordnungsbeispiel einer auslastungsbedingten Versagenswahrscheinlichkeit des Tf	97
Tabelle 21: Stufe der Bedrohungslage nach Angreifertyp in IEC 62443-3-3 [114]	102
Tabelle 22: Beispiel für eine 4 x 5-Manipulationsmatrix mit fünf qualitativen Skalenkategorien	104
Tabelle 23: Beispiel für die Zuweisung von qualitativer Skala zu den Faktorenwerten	105
Tabelle 24: Beispiel für eine Manipulationsmatrix mit der Zuordnung der Verstärkungsfaktoren	105
Tabelle 25: Berechnung der Konfrontationswahrscheinlichkeit am Beispiel von Deutschland	110
Tabelle 26: Mittlere planerische Streckenauslastung im Bereich der DB Netz AG nach [45, 95]	111
Tabelle 27: Beispiel einer Zuordnungstabelle von Betriebsdichte und Reduktionsfaktor	112
Tabelle 28: Kombination von Unfallart und Unfallbeteiligten	116
Tabelle 29: Klasse der Unfallgeschwindigkeit in der Bewertungssystematik	117
Tabelle 30: Opferzahl der ausgewählten Unfällen in der Geschwindigkeitsklasse 5 und 6	118
Tabelle 31: Unfallklasse und deren Opferzahl in der Bewertungssystematik	119
Tabelle 32: Grundparameter des Beispielszenarios	129
Tabelle 33: Parameter eines Störungsszenarios	131
Tabelle 34: Rechenbeispiel einer Konzeptvariante – Teil 1	133
Tabelle 35: Rechenbeispiel einer Konzeptvariante – Teil 2	133
Tabelle 36: Rechenbeispiel einer Konzeptvariante – Teil 3	135
Tabelle 37: Rechenbeispiel einer Konzeptvariante – Teil 4	136
Tabelle 38: Rechenbeispiel einer Konzeptvariante – Teil 5	138
Tabelle 39: Rechenbeispiel einer Konzeptvariante – Teil 6	139
Tabelle 40: Beispielberechnung des Betriebsrisiko pro Stunde	140
Tabelle 41: Beispielberechnung des Betriebsrisikos bei 72 Std. Betrieb	140
Tabelle 42: Rechenbeispiel des Qualitätsindex	142
Tabelle 43: Basisvariante 1	144
Tabelle 44: Basisvariante 2	145

Tabelle 45: Basisvariante 3	146
Tabelle 46: Basisvariante 4	147
Tabelle 47: Basisvariante 5	149
Tabelle 48: Basisvariante 6	150
Tabelle 49: Basisvariante 7	151
Tabelle 50: Basisvariante 8	152
Tabelle 51: Basisvariante 9	153
Tabelle 52: Basisvariante 10	154
Tabelle 53: Vergleich von Basisvarianten	155
Tabelle 54: Variantenablauf und Ergebnisse des Rückfallebenenkonzepts A	159
Tabelle 55: Variantenablauf und Ergebnisse des Rückfallebenenkonzepts B	160
Tabelle 56: Variantenablauf und Ergebnisse des Rückfallebenenkonzepts C	161
Tabelle 57: Variantenablauf und Ergebnisse des Rückfallebenenkonzepts D	163
Tabelle 58: Vergleich von Rückfallebenenkonzepten	164
Tabelle 59: Betriebliche Maßnahmen zur Erhöhung der Sicherheit und deren Konsequenzen	166
Tabelle 60: Betriebliche Maßnahmen zur Erhöhung des Leistungsniveaus und deren Konsequenzen	168
Tabelle 61: Betriebliche Maßnahmen zur Verbesserung der Verfügbarkeit und deren Konsequenzen	169

Tabellen, die keine Quellenangabe besitzen, wurden vom Autor persönlich erstellt.

1 Einleitung

Das System Eisenbahn ist ein hochkomplexes soziotechnisches Verkehrssystem mit einer Vielzahl von internen und externen Mensch-Maschine-Schnittstellen. Seit den 1990er Jahren werden im Eisenbahnwesen zunehmend neue Systeme mit Rechentechnik installiert. Dies hatte vielfältige Änderungen in den Systemarchitekturen, aber auch in der technischen Realisierung der betrieblichen Funktionalitäten zur Folge. Begleitet wurden diese technischen und betrieblichen Veränderungen durch systematische Betrachtungen zur Sicherheit und Verfügbarkeit der Systeme im Bahnbetrieb [1]. Wirft man einen Blick auf die Verkehrsunfallstatistik der vergangenen 50 Jahre, so wird man gleich feststellen können, dass sich das Eisenbahnsystem bisher als das sicherste Verkehrsmittel im Bereich Landverkehr bewährt hat. Durch die zunehmende Automatisierung und die verbreitete Anwendung von Informationstechnik (IT) im Eisenbahnwesen, wie in Abbildung 1 dargestellt wird, bekommt auch die Frage nach ausreichender und gewährleisteter IT-Security einen neuen und wichtigen Stellenwert [1, 2].

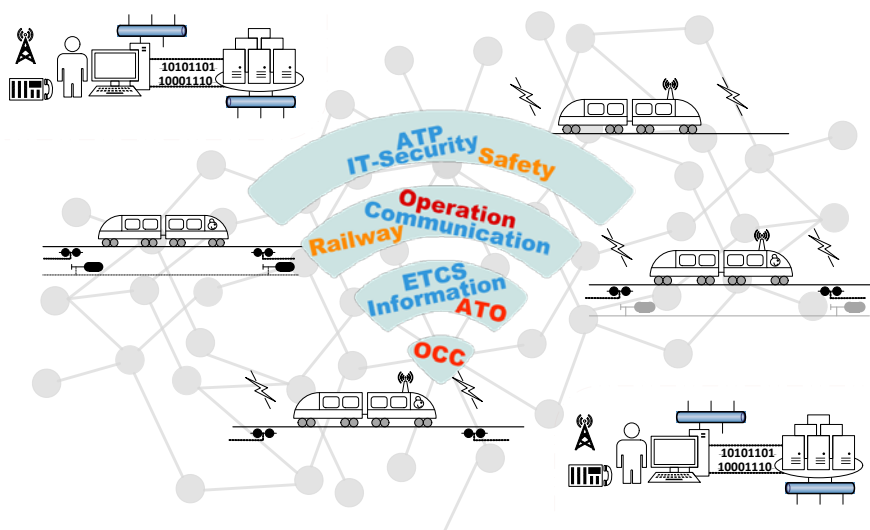


Abbildung 1: Verbreitete Anwendung von IT im Eisenbahnsystem

IT-Security, auch gängig als Cyber-Sicherheit oder IT-Sicherheit bekannt, hat die Aufgabe, das Schutzobjekt vor dem IT-Angriff zu schützen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt im Leitfaden Cyber-Sicherheits-Check die aktuelle Lage zum IT-Angriff: *“Cyber-Sicherheit, Cyber-Angriff, Cyber-Kriminalität und Cyber-Kriegsführung sind längst zu Schlagwörtern in Sicherheitsdiskussionen avanciert. [...] Der Mythos, dass es sich hierbei um Aktivitäten von Einzelnen mit einem Ausnahmewissen handelt, ist der Erkenntnis gewichen, dass Cyber-Sicherheit eine wichtige Facette der Sicherheit ist und diese durch die Leitung / das Management einer Institution berücksichtigt werden muss.“* [3] Durch den erstmalig im Juni 2010 bekanntgegebenen IT-Angriff „Stuxnet“ auf ein Siemens S7 Steuerungssystem hat sich gezeigt, dass auch ein isoliertes, industrielles

Automatisierungssystem in einem begrenzten, kontrollierten Gelände nicht vor einem beabsichtigen IT-Angriff sicher ist [4].

Bis heute wurde über IT-Angriffe auf das Eisenbahnsystem nur wenig berichtet. Im Folgenden werden einige Beispiele erwähnt: Im Jahr 2003 wurde die Zentrale des CSX-Railway im amerikanischen Bundesstaat Florida vom Virus „Sobig“ angegriffen und das Signalsystem wurde lahmgelegt [5]. In der polnischen Stadt Lodz hat es im Jahr 2007 einen Vorfall gegeben: Ein 14-jähriger Junge hat sich mit einer selbst modifizierten Fernsehsteuerung in die Straßenbahnweiche eingehackt und daran herumgespielt. Dadurch sind vier Straßenbahnen entgleist und 12 Fahrgäste verletzt worden [6]. Im Jahr 2011 gab es wieder einen Bericht über einen Angriff auf einen Computer der Northwest Rail in den USA. In dessen Folge wurde die Signalisierung zwei Tage lang gestört [7]. Bei dem Angriff „WannaCry“ im Mai 2017 sind dem Bericht zufolge weltweit über 200.000 Rechner infiziert worden. Auch Teile des nicht-sicherheitsrelevanten Systems der Deutschen Bahn, wie z. B. die Anzeigen der Fahrgastinformation, Kameras und Ticketautomaten, waren betroffen, wie in Abbildung 2 gezeigt wird [8]. Die potenzielle Bedrohung durch IT-Security-Angriffe steigt ständig weiter und die schnell wachsende digitale Infrastruktur hat dazu beigetragen, dass die Anzahl der Angriffspunkte erhöht wird. Im Oktober 2018 gab das Bundesamt für Sicherheit in der Informationstechnik (BSI) erneut Warnungen heraus und sprach von einer neuen Dimension der flexiblen und professionellen Hackerangriffe, deren Fokus zunehmend auf die Kritische Infrastruktur in Deutschland gerichtet ist [9].



Abbildung 2: Von Ransomware WannaCry betroffenen Fahrgastanzeige im Mai 2017 [8]

Durch das Inkrafttreten des IT-Sicherheitsgesetzes im Juli 2015 ist die Beschäftigung mit dem Thema IT-Security für Kritische Infrastruktur wie die deutschen Bahnen und die Bahnindustrie auch rechtlich notwendig geworden. Das IT-Sicherheitsgesetz fordert in §8a (1): „*Betreiber Kritischer Infrastrukturen sind verpflichtet, [...] angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich*

sind.“[10] Die Forderung des Gesetzes hat nicht unerhebliche Auswirkungen, da erstmals konkret die Bedrohung durch ein Nichtfunktionieren der Informationstechnik angesprochen wird und entsprechende Maßnahmen gegen dessen Auswirkungen gefordert werden.

Durch die zunehmende Digitalisierung und IT-Vernetzung sowie die rasanten Fortschritte der Entwicklung der IT werden die technischen Systeme zwar immer moderner und intelligenter, jedoch wird das System zugleich durch das steigende und in sich wachsende IT-Umfeld immer angreifbarer. Die Bedeutung einer Bedrohung der IT-Security und ihre Auswirkung auf den Bahnbetrieb ist den Fachleuten mittlerweile durch die gesetzlichen Anforderungen und die IT-Security-Vorfälle der Vergangenheit sehr bewusst. Unabhängig von den getroffenen Vorkehrungen muss davon ausgegangen werden, dass nicht jeder Angriff tatsächlich festgestellt und abgewendet werden kann. Dies bedeutet u. a., dass der Bahnbetrieb eingehender zu betrachten ist, da ein vermuteter oder tatsächlicher IT-Security-Angriff dazu führen kann, dass das System der Bahn teilweise oder ggf. komplett in der Rückfallebene betrieben wird. Es ist aber keine Option, den Bahnbetrieb bei vermuteten oder erfolgreichen Angriffen stets stillzulegen. Dies ist sowohl wirtschaftlich unsinnig als auch widersprüchlich zum IT-Sicherheitsgesetz, welches die Aufrechterhaltung der Funktionsfähigkeit der Kritischen Infrastruktur ausdrücklich fordert.

Allerdings enthält das heutige Rückfallebenenkonzept von beispielsweise der Deutschen Bahn AG keine konkreten Aussagen zum Bahnbetrieb nach IT-Security-Angriffen. Das heutige Rückfallebenenkonzept des Bahnbetriebs ist dafür vorgesehen, die bisher anzunehmenden betrieblichen Einschränkungen, welches in der Regel nur Safety-Ereignisse und deren Folgen sind, zu beherrschen. Dabei kann es sich z. B. sowohl um zufällige technische Störungen als auch um die Beherrschung von Naturereignissen handeln. Wird jedoch der Kreis der möglichen Ursachen um den IT-Angriff erweitert, ist zu erwarten, dass eine Anpassung und Erweiterung des Rückfallebenenkonzepts notwendig werden, die den Charakteristiken eines IT-Security-Angriffs Rechnung tragen. Wird berücksichtigt, dass ein erfolgreicher IT-Security-Angriff die Funktionsfähigkeit einer Kritischen Infrastruktur durchaus signifikant einschränken kann, so fallen IT-Security-Angriffe als vorsätzliche Handlungen formal in jedem Fall in den Geltungsbereich des Krisenmanagements. Zum Krisenmanagement für die Betreiber Kritischer Infrastrukturen existiert vielfältige nationale und internationale Literatur. In Deutschland kann beispielsweise auf die Veröffentlichungen des Bundesministeriums des Innern, für Bau und Heimat (BMI) [11–13] verwiesen werden. Auch Normen, die sich mit dem Thema Betriebliche Kontinuität bzw. Aufrechterhaltung der Betriebsfähigkeit beschäftigen, sind verfügbar [14–16]. Im Bereich Eisenbahn existiert bei einem Netzbetreiber wie der Deutschen Bahn AG auch eine entsprechende Strukturrichtlinie zum Krisenmanagement in den Betriebszentralen mit dem Fokus auf die Betriebsleitungen [17]. Es muss jedoch hinterfragt werden, inwieweit die herkömmliche Vorgehensweise zum Krisenmanagement sowie die Pläne auf solch einer hohen Abstraktionsebene bei der Betriebsfortführung nach IT-Security-Angriffen tatsächlich anwendbar sind. Die dazu notwendige Rückfallebene entspricht nicht denen, die als Reaktion auf herkömmliche Krisen zum Einsatz kommen, da den Besonderheiten von IT-Angriffen nicht

Rechnung getragen wird. Darüber hinaus geht es bei dem Krisenmanagement vornehmlich um den Aufbau der Organisationsstruktur und Organisationskommunikation, die aber bei der tatsächlichen Funktionsfortführung eines Rückfallebenenkonzepts nicht direkt relevant sind.

Das System Bahn als Kritische Infrastruktur hat nicht nur die Aufgabe, Personen und Güter sicher zu transportieren, sondern auch, die Funktionalität und Stabilität der Gesellschaft durch ein hohes Leistungsniveau und eine hohe Verfügbarkeit des Bahnbetriebs zu gewährleisten. Mit der immer ernster zu nehmenden Bedrohungslage der IT-Security-Angriffe auf die Kritische Infrastruktur stellt sich auch die Frage zum künftigen Bahnbetrieb unter der IT-Angriffsbedrohung:

- Erstens: Wie gut lässt sich die Betriebsqualität der Bahn bezüglich der Sicherheit, dem Leistungsniveau und der Verfügbarkeit bei einem herkömmlichen Störfall sowie im Fall eines erfolgreichen bzw. vermuteten IT-Security-Angriffs erbringen?
- Zweitens: Wie lässt sich die Betriebsqualität des Rückfallebenenkonzepts systematisch analysieren, bewerten und vergleichen, wenn neben der systemtechnischen Auslegung auch dem dynamischen IT-Umfeld, den Charakteristiken des IT-Angriffs sowie die Rolle der Menschen angemessen Rechnung getragen wird?
- Letzteres: Durch welche Prinzipien lässt sich das Rückfallebenenkonzept des Bahnbetriebs unter der IT-Angriffsbedrohung künftig gestalten, damit die Bahn ihre Aufgabe als Kritische Infrastruktur gemäß der gesellschaftlichen Erwartung möglichst erreichen kann?

Um die Qualitäten des Rückfallebenenkonzepts systematisch analysieren, bewerten und miteinander vergleichen zu können, steht im Mittelpunkt dieser Arbeit die Schaffung einer generischen, risikoorientierten Systematik zur Bewertung eines heutigen und künftigen Rückfallebenenkonzepts mit dem Ziel, das dynamische IT-Umfeld, die Charakteristiken des IT-Angriffs, die Menschen und die systemtechnischen Auslegung der Rückfallebene zusammenhängend berücksichtigen zu können.

Wie in Abbildung 3 gezeigt wird, beginnt die Arbeit nach diesem allgemeinen Einleitungskapitel gleich in Kapitel 2 mit einer taxonomischen Einteilung von Safety, Security und deren Auswirkungen auf den Bahnbetrieb. Es folgt eine ausführliche Behandlung von Charakteristiken des IT-Security-Angriffs. Insgesamt werden 5 primäre Charakteristiken analysiert, welche im Vergleich zu den Safety-Ereignissen deutliche Unterschiede aufweisen. Dies sind die Wahrscheinlichkeit, die Offenbarung, das Ausmaß, die Priorität und die Dauer. Anschließend werden die elementaren Aufgaben der Bahn als Kritische Infrastruktur und deren Anforderungen an die Rückfallebene aus funktionalen, gesellschaftlichen und rechtlichen Aspekten eingehend hergeleitet. Abschließend folgt eine Vorstellung eines Rückfallebenenkonzepts, in der das Rückfallebenenkonzept aus Sicht des Systemprozesses, der Tätigkeiten und des Strukturprinzips systematisch behandelt wird.

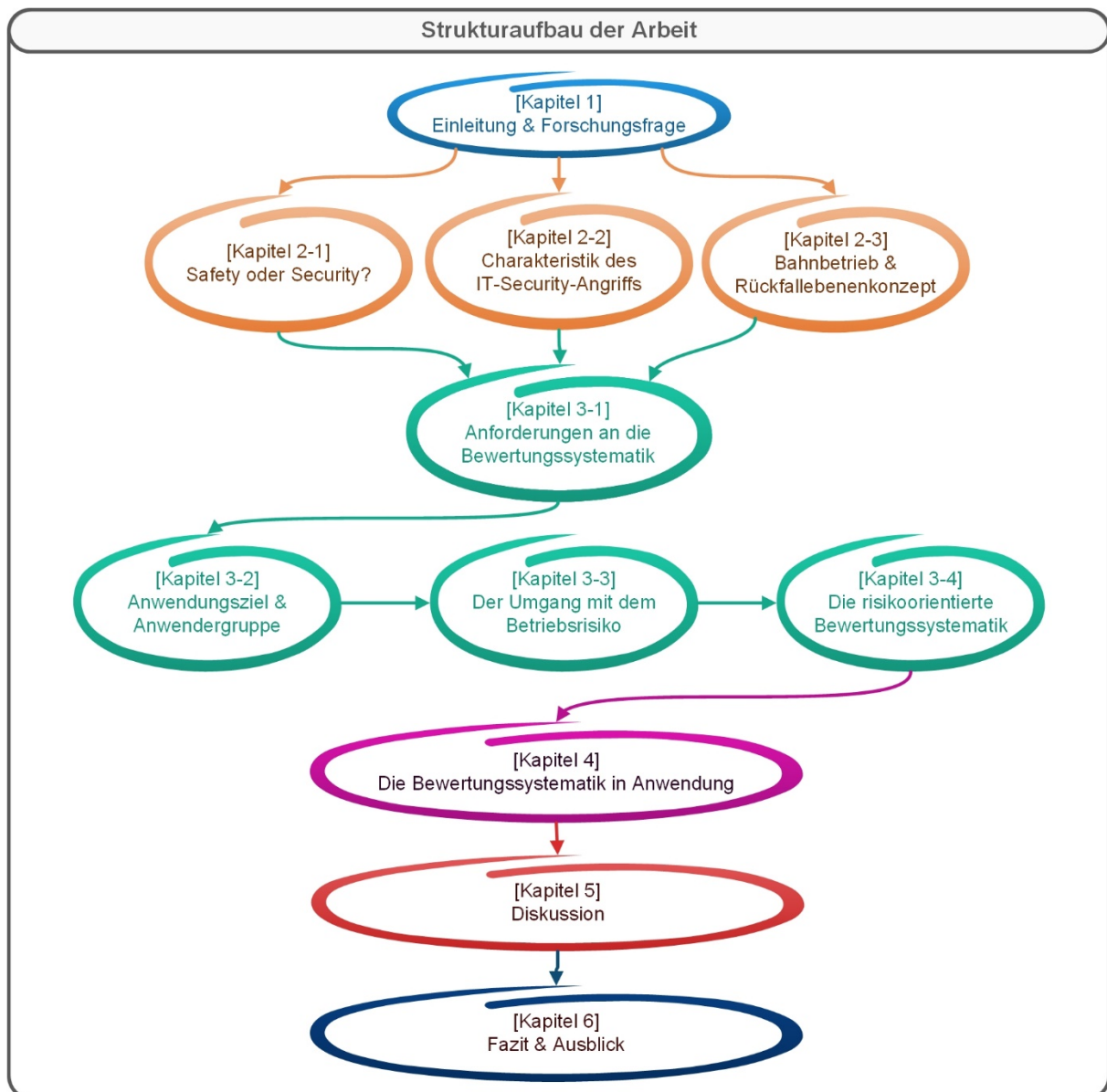


Abbildung 3: Strukturaufbau der Arbeit

Mit der Analyse der Herausforderung des künftigen Bahnbetriebs in der Rückfallebene im Hinblick auf die Rolle der Menschen und die Charakteristiken des IT-Security-Angriffs beginnt die Arbeit in Kapitel 3. Nach dem Ergebnis der Analyse werden die Anforderungen an die Bewertungssystematik systematisch abgeleitet. Es folgt anschließend eine ausführliche Abhandlung über den Kontext, den Grenzwert und die Anwendung des Betriebsrisikos in der Bewertungssystematik. In diesem Zusammenhang wird auch das Konzept Risiko-Budgetierung zur proaktiven Steuerung der Entwicklung des Betriebsrisikos vorgestellt. Am Schluss des Kapitels werden die Strukturteile und die Ergebnisteile der risikoorientierten Bewertungssystematik im Einzelnen behandelt.

Anschließend wird in Kapitel 4 der Ablauf der Anwendung anhand eines Beispiels demonstriert. Der Ablauf der Anwendung wird in vier Phasen aufgeteilt. Er beginnt mit der Festlegung der grundlegenden Parameter und dem Bestimmen des Störungsszenarios. Es folgt

das Konzipieren von Varianten und das Ermitteln von deren Qualität. Am Ende wird das Rückfallebenenkonzept aus den Varianten strategisch gestaltet. Aufgrund der Komplexität des Bahnsystems sowie einer Vielzahl unterschiedlicher Betriebsszenarien steht eine umfassende Untersuchung und Weiterentwicklung eines Rückfallebenenkonzepts nicht im Kontext dieser Arbeit.

Vor dem Schluss dieser Arbeit wird in Kapitel 5 eine Diskussion über die Maßnahmen zur Erhöhung der Betriebsqualität sowie das Konzept einer temporären Räumungsprüfstelle gegeben. Die Arbeit schließt in Kapitel 6 mit einer Zusammenfassung der wesentlichen Forschungsergebnisse und einem spannenden Ausblick in den zukünftigen Forschungsbedarf ab.

2 IT-Security und Bahnbetrieb

2.1 Safety oder Security?

Der mehrdeutige deutsche Begriff „Sicherheit“ umfasst mindestens zwei Themenbereiche, welche in der englischen Sprache als „Safety“ und „Security“ unterschieden werden. Im allgemeinen Verständnis der deutschen Sprache hat „Sicherheit“ nach DUDEN die Bedeutung: „Zustand des Sicherseins vor Gefahr oder Schaden.“ [18] D. h.: Ist jemand oder etwas im Zustand des Sicherseins, kann dies allgemein sprachlich beispielsweise wie folgt ausgedrückt werden: „Sie sind jetzt in Sicherheit“, „Sie sind jetzt sicher“ auf Deutsch oder „You are safe now“ auf Englisch. Auch in vielen Bereichen des Ingenieurwesens und der Ingenieurwissenschaften ist der Begriff „Sicherheit (safe)“ neutral und beschreibt, wie in der allgemeinen Sprache, lediglich einen Zustand des Sicherseins. Der Unterschied ist, dass die Definition der Sicherheit im Bereich des Ingenieurwesens mittelbar durch das Konzept „Risiko“ ausgedrückt wird. Z. B. kann die Definition der „Sicherheit (safe)“ im Ingenieurwesen aus [19–21] wie folgt zusammengefasst werden: „Sicherheit ist das Freisein / das Nichtvorhandensein / die Abwesenheit von unvermeidbaren / nicht akzeptierbaren Schadensrisiken.“ Tatsächlich gibt es für das Konzept „Risiko“ unterschiedliche Definitionen, jedoch kann im Bereich Eisenbahn die gleiche Definition nach EN 50126-2 weitgehend durchgesetzt werden, in der das Risiko als *„Kombination aus erwarteter Häufigkeit eines Schadens und erwartetem Schweregrad dieses Schadens“* definiert wird [22]. Die mittelbare Betrachtung der Sicherheit durch unvermeidbare / nicht akzeptierbare Schadensrisiken berücksichtigt die Tatsache, dass in der Regel z. B. aus technischen oder wirtschaftlichen Gründen nur ein bestimmtes Niveau der Sicherheit erreicht werden kann, nicht aber die absolute und dauerhafte Sicherheit. Demzufolge ist jemand / etwas in Sicherheit, solange das vorhandene Risiko ein bestimmtes Niveau, welches auch als Risikogrenzwert bekannt ist, nicht überschreitet.

Ausgehend vom Konzept „Risiko“, in dem noch keine Details über die Charakteristiken bzw. die Ursachen eines Ereignisses enthalten sind, wird Safety / Security meistens als Differenzierung bzw. Spezifizierung der Eigenschaften eines Ereignisses angesehen. Im Allgemeinen werden die Ereignisse bzw. deren Ursachen oder Konsequenzen, die unbeabsichtigt und zufällig entstanden sind, mit „Safety“ in Verbindung gebracht. Im Gegensatz dazu werden die Ereignisse bzw. deren Ursachen oder Konsequenzen, die beabsichtigt und böswillig herbeigeführt werden, als „Security“ eingeordnet [1, 2, 21, 23–27]. Im heutigen Eisenbahnsystem, vor allem in den Bereichen Systemzuverlässigkeit und sicherheitsrelevante Funktionen, hat „Safety“ die Aufgabe, das System zum Beispiel vor unbeabsichtigten, zufälligen Fehlfunktionen bzw. Funktionsversagen zu schützen. „Security“ sichert das System zum Beispiel vor unberechtigtem Zutritt bzw. beabsichtigten, böswilligen Angriffen [21, 27].

Es ist zu beachten, dass „Safety“ und „safe“ in dem englischen sprachlichen Gebrauch meistens die gleiche Bedeutung haben [28]. Um die Begrifflichkeiten klar zu unterscheiden, wird im Rahmen dieser Arbeit „Sicherheit / sicher“ auf Deutsch und „safe“ auf Englisch als der Zustand des Sicherseins verstanden, der durch das Konzept „Risiko“ dargestellt wird. „Safety“ und „Security“ sind dann zwei Arbeitsfelder: Das eine beschäftigt sich mit den unbeabsichtigten Ereignissen und das andere mit den beabsichtigten Ereignissen. Anforderungen, Maßnahmen sowie weitere Aktivitäten, die den jeweiligen Arbeitsbereichen zufallen, können entsprechend z. B. durch folgende Bezeichnungen spezifiziert werden: Safety-Maßnahme, Security-Maßnahme, Safety-Anforderung oder Security-Anforderung.

Allerdings ist in manchen Fällen nicht möglich, festzustellen, ob ein beobachtetes Ereignis beabsichtigt oder unbeabsichtigt ausgelöst wurde (siehe Kapitel 2.2.2 fürs Detail). Solche Ereignisse werden hier als unbekanntes Ereignis klassifiziert. Egal, ob die Ursache eines Ereignisses Safety, Security oder unbekannt ist: Solange die Folge eines Ereignisses durch bestimmte Anzeichen im Betrieb offenbart werden kann, sind diese als betriebliche Ereignisse zu behandeln. Jedoch werden nicht alle betrieblichen Ereignisse den aktuellen Bahnbetrieb akut beeinträchtigen. Zum Beispiel kann der Bahnbetrieb aufgrund einer technischen Redundanz mit Hot-Standby ohne unmittelbare Beeinträchtigung reibungslos weiter fortgeführt werden, auch wenn die Störung eines technischen Systems eingetreten ist. Lediglich ein Ereignis mit akuter Beeinträchtigung verursacht eine Unregelmäßigkeit im Bahnbetrieb und bringt negative Folgen in die aktuelle Betriebslage. Um feststellen zu können, ob sich ein Ereignis tatsächlich bis zur Beeinträchtigung des aktuellen Bahnbetriebs weiterentwickeln kann, sind neben den identifizierten Ereignissen z. B. auch die aktuelle Betriebslage, das aktuelle Betriebskonzept und die Systemauslegung gemeinsam zu betrachten.

Wie die Abbildung 4 zeigt, kann sich diese Unregelmäßigkeit im Bahnbetrieb im Laufe des Betriebsablaufs entweder zur Betriebsabweichung oder Betriebsgefahr weiterentwickeln. Die Betriebsabweichung umfasst die Zustände Betriebsstörung und Betriebshemmung. Im Rahmen dieser Arbeit beschreibt die Betriebsstörung den Zustand, in dem der Bahnbetrieb nach dem Eintreten eines Ereignisses bei einer fehlenden aktiven Handlung nach dem Fail-safe-Prinzip zum Stillstand kommen und mit einer ungewissen Zeitdauer in diesem Zustand bleiben kann. Wenn sich zum Beispiel ein Hauptsignal mit absolutem Halt nicht mehr auf Fahrt stellen lässt, dann sollte ein Zug vor dem Signal solange stillstehen, bis die Rückfallebene für die Weiterfahrt eingeführt ist.

Im Gegensatz dazu umfasst die Betriebshemmung die Situation, in der der Bahnbetrieb nach dem Eintreten eines Ereignisses nicht zwingend zum Stillstand kommen muss, die jedoch zur Gewährleistung der Betriebsqualität angemessene Handlung bzw. die Rückfallebene eingeführt werden sollte. Als Beispiel wird der Bahnbetrieb bei einer Windwarnung zwar nicht zwingend zum Stillstand kommen, die höchstzulässige Geschwindigkeit sollte aber aus Sicherheitsgründen herabgesetzt werden. Neben der Betriebsabweichung kann sich ein Ereignis im Bahnbetrieb auch zu Betriebsgefahr weiterentwickeln, die dann entweder mit einem Unfall oder einem Beinahunfall endet. Sowohl die Betriebsabweichung als auch die Betriebsgefahr

hat einen Schaden als Folge. Dieser Schaden kann in unterschiedlichen Formen auftreten, z. B. als Personenschaden, Sachschaden, Vermögensschaden oder Imageschaden. Durch die Zusammenstellung der taxonomischen Übersicht in Abbildung 4 wird gezeigt, dass sowohl Safety-Ereignisse als auch Security-Ereignisse aus betrieblicher Sicht zu Unregelmäßigkeiten im Betrieb und in der Anwendung von Rückfallebenen führen können. Zur Gewährleistung der Betriebsqualität in der Rückfallebene müssen daher die Safety-Ereignisse und die Security-Ereignisse in ihrer Gesamtheit gemeinsam betrachtet werden.

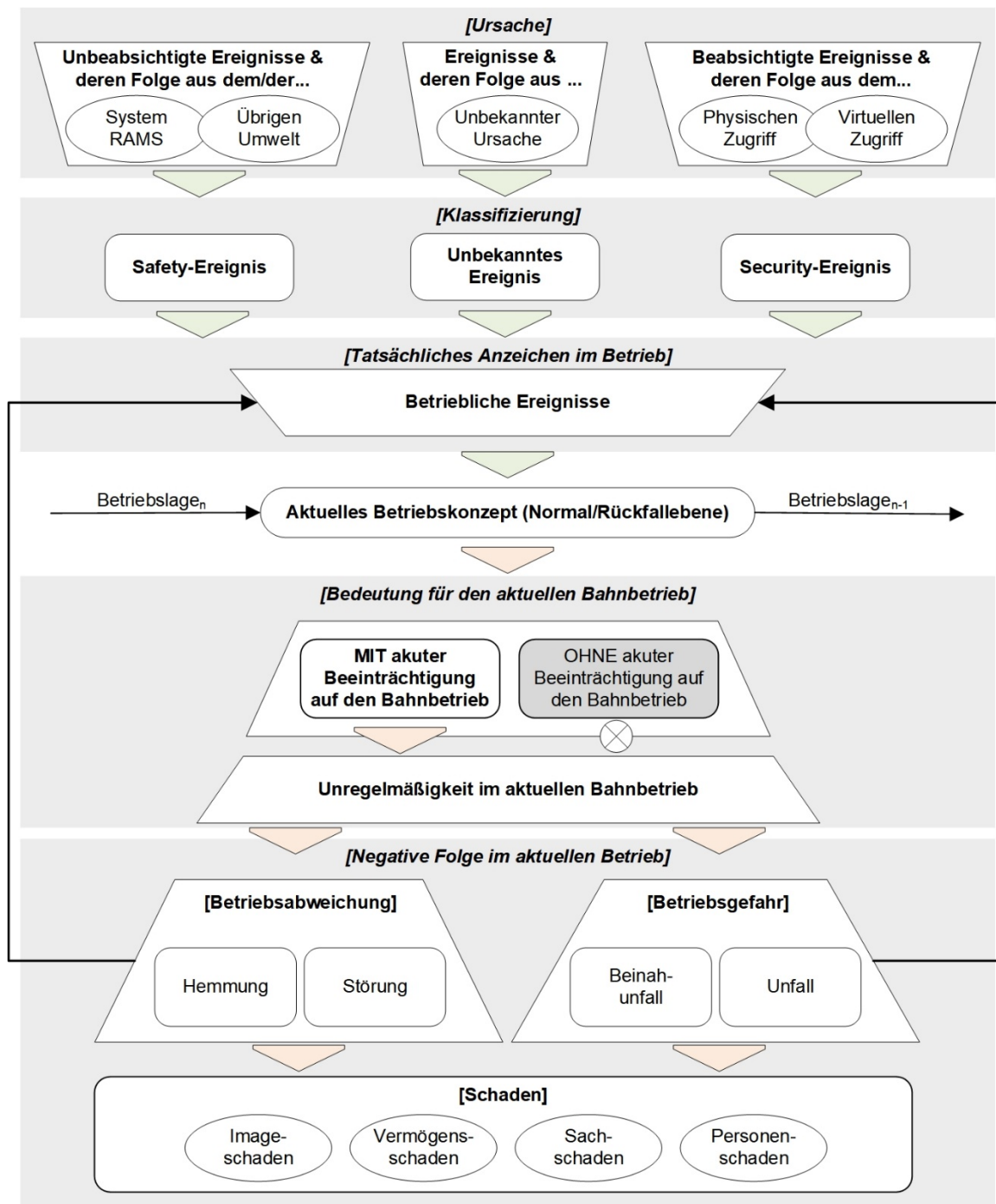


Abbildung 4: Eine taxonomische Übersicht von Safety, Security und deren Folge auf Bahnbetrieb

2.2 Die Charakteristik des IT-Security-Angriffs

IT-Security, auch gängig als Cyber-Security bekannt, gehört zu dem Aufgabenfeld der allgemeinen Informationssicherheit, in dem die Informationen jeglicher Art, egal ob auf Papier, in IT-Systemen oder im Gedächtnis der Menschen, gegen beabsichtigte und unbeabsichtigte Ereignisse zu schützen sind. Die grundlegenden Schutzziele der Informationssicherheit sind die Aufrechterhaltung der Integrität, Vertraulichkeit und Verfügbarkeit der Informationen, einschließlich der darauf basierenden Kommunikation, Anwendungen, Prozesse und verarbeiteten Informationen [29]. Je nach Anwendungsfall kann auf ein bestimmtes Schutzziel verzichtet werden oder können auch weitere Schutzziele wie Authentizität, Zurechenbarkeit oder Nicht-Abstreitbarkeit der Informationen in Betracht gezogen werden [29–31]. Zum Beispiel hat die Vertraulichkeit von Informationen, die öffentlich verfügbar sind, als Schutzziel keine Bedeutung. Dafür müssen aber z. B. die Authentizität und Integrität je nach Inhalt der Informationen sichergestellt werden. Als Teilgebiet der Informationssicherheit beschäftigt sich IT-Security ausschließlich mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung in IT-Systemen vor beabsichtigten böswilligen Angriffen [29].

Informationen, die in dem IT-System vorhanden sind, können durch einen Angriff z. B. zerstört, verändert oder offengelegt werden. Um die Informationen in einem IT-System zu zerstören, kann sich ein Angreifer beispielsweise einen unautorisierten, physischen Zugang zu dem IT-System beschafft haben und kann anschließend mit physischer Gewalt das Speichermedium des IT-Systems zerstören. Auch wenn der Angreifer keinen direkten Angriff auf die elektronisch gespeicherte Information in einem IT-System ausgeübt hat, ist die Information in dem IT-System durch diesen physischen Angriff gleichermaßen zerstört worden. Als Alternative kann ein Angreifer auch ein Schadprogramm in dem IT-System installieren, nachdem er den unautorisierten, physischen Zugang zu dem IT-System erlangt hat, und die Information durch das Schadprogramm zerstören lassen. Falls das Ziel-IT-System mit den anderen IT-Systemen vernetzt ist, kann der Angreifer die Information in dem Ziel-IT-System auch ganz ohne den physischen Zugang zu dem Angriffsziel, sondern virtuell über ein IT-Netzwerk zerstören bzw. zerstören lassen. Das bedeutet, dass der IT-Angriff eine Spezifizierung der Angriffsart auf IT-Systeme ist, in der der Angriff auf elektronisch gespeicherte Informationen und deren Verarbeitung nicht direkt durch physische Gewalt, sondern virtuell über IT-Systeme stattfindet. Dies beinhaltet auch den Fall, dass der Angreifer sich erst den Zugang zu dem Ziel-IT-System bzw. zu Umsystemen beschafft hat und den Angriffsvorgang anschließend virtuell auf das Ziel-IT-System ausübt.

In diesem Abschnitt werden 5 Charakteristiken eingehend diskutiert, welche im Vergleich zu den Safety-Ereignissen einen deutlichen Unterschied aufweisen. Dies sind die Wahrscheinlichkeit, die Offenbarung, das Ausmaß, die Priorität und die Dauer eines IT-Security-Angriffs.

2.2.1 Wahrscheinlichkeit

Im Trend der Automatisierung und der Digitalisierung werden die Alltagsgegenstände der End-Benutzer, die Office-IT der Betreiber sowie die Industrieanlagen der Betreiber durch IT zunehmend miteinander direkt oder indirekt verbunden. Die Vernetzung von IT-Systemen führt dazu, dass sich die Anzahl der Umsysteme eines IT-Systems dynamisch vergrößert und zugleich mehr potenzielle Zugangspunkte für den Angreifer erschaffen werden. Dies hat gravierende Konsequenzen auf die Sicherheit bzw. auf das Risiko eines Systems. Wie bereits beschrieben, beruht das Risiko eines Systems auf der Häufigkeit oder Wahrscheinlichkeit des Eintretens eines spezifischen Ereignisses. Zum Festlegen der Wahrscheinlichkeit der Safety-Ereignisse, die unbeabsichtigt und zufällig entstanden sind, stehen heutzutage meistens belastbare Statistiken über Jahrzehnte oder Untersuchungsberichte zur Verfügung. Die Wahrscheinlichkeit oder Häufigkeit des Eintretens von Safety-Ereignissen sowie deren Konsequenzen sind durchaus einschätzbar, da das Umfeld, in dem die Ereignisse sich befinden, über Jahrzehnte hinweg quasi stabil ist [2]. Das bedeutet, dass das Niveau der Sicherheit bzw. das vorhandene Risiko des Systems, in dem lediglich Safety-Ereignisse betrachtet wurden, nach dessen Inbetriebnahme bis zum Ende der Systemlebensdauer in der Regel stabil bleibt. Voraussetzung dafür ist jedoch, dass die planmäßigen Inspektionen und Instandhaltungen korrekt durchgeführt wurden.

Im Gegensatz dazu ist die Wahrscheinlichkeit oder Häufigkeit des Eintretens von Security-Ereignissen bzw. eines Angriffs grundsätzlich nicht genau einschätzbar. Das Eintreten eines Security-Ereignisses hängt wesentlich von z. B. der Motivation, der Fähigkeit, den Ressourcen, der Genialität und der Beharrlichkeit des Angreifers ab, für den bisher keine belastbare Statistik vorliegt und die es mit der höchsten Möglichkeit auch nicht geben wird. Dazu muss bei dem Thema IT-Angriff beachtet werden, dass sich nicht nur die Fähigkeit des Angreifers und dessen Angriffsmethode mit der rasanten technischen Entwicklung ständig weiter entwickeln werden, sondern auch dessen IT-Umgebung verändert sich bzw. wächst wegen der zunehmenden Digitalisierung und Vernetzung ebenfalls dynamisch. Dies führt dazu, dass die Bedrohung durch einen IT-Angriff mit der Entwicklung der IT-Vernetzung ständig ansteigt. Das hat auch zur Folge, dass sich das Niveau der Sicherheit bzw. das vorhandene Risiko eines Systems, welches zum Zeitpunkt der Inbetriebnahme ermittelt wurde, im Umfeld der wachsenden IT-Umgebung während der Systemlebensdauer ebenfalls dynamisch verändern werden. Diese dynamische Änderung der IT-Umgebung stellt für die heutige Kritische Infrastruktur eine große Herausforderung dar, da sie ihre Funktionsfähigkeit einschließlich Sicherheit, Leistung und Verfügbarkeit in dieser dynamisch wachsenden Umgebung stets in Stand halten muss.

Dennoch ist das Worst-Case-Szenario, in dem eine sicherheitsrelevante Funktion von einem Angreifer komplett kompromittiert und übernommen wurde, angesichts der Komplexität und des Designs der sicherheitsrelevanten Systeme sowie der vorgesehenen Aufrüstung von entsprechenden Security-Maßnahmen zwar nicht undenkbar, aber die Wahrscheinlichkeit, dass z. B. im Eisenbahnbetrieb die Signalabhängigkeit komplett aufgehoben wird und alle Hauptsignale gleichzeitig auf Fahrt gehen, ist eher gering. Wie in [32] ausgeführt, besteht eine

größere Gefahr darin, dass durch die IT-Angriffe das System gestört wird. Da die Häufigkeit des Eintretens von Safety-Ereignissen stabil ist, wird sich die Häufigkeit des Eintretens von gesamten vergleichbaren Ereignissen, bei deren Eintreten eine Betriebsstörung des Systems herbeigeführt wird, angesichts der in sich wachsenden IT-Umgebung und der ansteigenden IT-Angriffe ebenfalls erhöhen.

2.2.2 Offenbarung

IT-Angriffe können sehr unterschiedliche Auswirkungen haben. Sie können unbemerkt bleiben und lediglich zur Datenermittlung gewonnen werden. Sie können auch die Integrität von sicherheitsrelevanten Informationen verletzen und das Versagen sicherheitsrelevanter Funktionen könnte bedeutsame Schäden materieller oder menschlicher Art zur Folge haben [33]. Beispielweise könnte die Fahrerlaubnis beim automatisierten Bahnbetrieb im Fall eines erfolgreichen IT-Angriffs während der Übertragung manipuliert und die Geschwindigkeitseinschränkung durch den Angreifer aufgehoben werden, wodurch eine Entgleisung des Zuges wegen überhöhter Geschwindigkeit herbeigeführt werden könnte. Jedoch könnte das gleiche gefährliche Ereignis, wenn auch theoretisch mit sehr geringer Wahrscheinlichkeit, ebenfalls durch einen zufälligen, unbeabsichtigten Übertragungs- oder Verarbeitungsfehler des IT-Systems entstanden sein. Es kann davon ausgegangen werden, dass sich Safety-Ereignisse und Security-Ereignisse in vielen Fällen durch vergleichbare Anzeichen, z. B. durch Störung, Hemmung oder durch einen Unfall, offenbaren. Ungeachtet deren Ursache wurden heutzutage bereits bei vielen sicherheitsrelevanten Systemen, wie auch bei dem System Bahn, viele ausgereifte, zuverlässige technische sowie betriebliche Maßnahmen implementiert, um eine rechtzeitige bzw. zeitnahe Offenbarung solcher Ereignisse zu ermöglichen.

Ob eine Unregelmäßigkeit im Betrieb tatsächlich durch einen IT-Angriff oder durch ein Safety-Ereignis verursacht wurde, lässt sich meist nicht eindeutig zuordnen. Dem Bericht zufolge brauchte eine Firma im Jahr 2016 im Durchschnitt 49 Tage [34] bzw. 99 Tage [35], um zu erkennen, dass ihr eigenes System das Opfer eines IT-Angriffs geworden ist. Nach der Entdeckung kann trotzdem nicht sichergestellt werden, ob alle Unregelmäßigkeiten im Bahnbetrieb, die in den Zeiten vor oder nach der Offenbarung aufgetreten sind, tatsächlich auf die IT-Angriffe allein zurückzuführen sind. Wichtig ist jedoch, dass die Maßnahmen gegen IT-Angriffe bis heute bei vielen Systemen oder Firmen nicht standardmäßig bzw. nicht nach dem Stand der Technik implementiert wurden. Auch für viele sicherheitsrelevante Systeme, wie z. B. die Eisenbahn in Deutschland, ist eine Implementierung angemessener Maßnahmen gegen IT-Angriffe erst nach dem Inkrafttreten des IT-Sicherheitsgesetzes im Juli 2015 obligatorisch geworden.

Wie in [1] berichtet wird, steht im Mittelpunkt der heutigen Aktivitäten der Bahn-IT-Security zumeist die Zusammenstellung von Anforderungen bzw. die Schaffung eines IT-Security-Management-Systems, das sich, vereinfacht ausgedrückt, mit dem Überwachen, Sammeln und Auswerten von Daten beschäftigt. Ein weiterer Schwerpunkt der Arbeiten liegt im Systemdesign, also in der Ableitung von Strukturen und Architekturen, welche neue Systeme

und Kommunikationsstrukturen möglichst vor IT-Angriffen schützen sollen. Das Ziel in dieser Tätigkeit ist es, Systeme so zu entwickeln und zu unterhalten, dass möglichsalle Angriffe erkannt und erfolgreich verhindert werden können. Allerdings sind die heutigen Systeme häufig nicht in der Lage, bei ihrer Implementierung von Gegenmaßnahmen mit der Geschwindigkeit des Anstiegs der IT-Bedrohung mitzuhalten. Wären die Schutzmaßnahmen des Systems dem Angreifer stets einen Schritt voraus, würde es keine erfolgreichen IT-Angriffe geben. Es ist aber davon auszugehen, dass sich diese Tatsache in der Zukunft mit großer Wahrscheinlichkeit wenig verändern wird und dadurch die Entwicklung der IT-Bedrohung der Implementierung der entsprechenden Gegenmaßnahmen immer einen Schritt voraus bleibt. Außerdem ist zu beachten, dass die Gefahr besteht, dass, je besser ein System durch Maßnahmen gegen Safety- sowie Security-Ereignisse geschützt ist, es desto sensativer auf kleine Zustandsabweichungen reagiert. Dies hat dann wiederum die negative Konsequenz, dass die Betriebsführung in der Gesamtheit noch häufiger als heute in der Rückfallebene zu erfolgen hat.

2.2.3 Ausmaß

Neben der steigenden Anzahl von Ereignissen, die die Verfügbarkeit des Systems beeinträchtigen können, hat die Entwicklung der wachsenden IT-Vernetzung unfreiwillig auch eine neue Verbindung zwischen den Angreifern und den potenziellen Opfern hergestellt. Dadurch zeigt sich hier bezüglich des Ausmaßes ein weiterer gravierender Unterschied zwischen der potenziellen Auswirkung eines Safety-Ereignisses und eines IT-Angriffs. Bei dem traditionellen Safety-Ereignis ist die Größe des betroffenen Bereichs bzw. die Anzahl des betroffenen Systems in der Regel sehr begrenzt. Z. B. kann im Eisenbahnbetrieb ein Blocksignal gestört sein und daher nicht mehr auf Fahrt gestellt werden oder eine Gleisfreimeldeanlage ausgefallen sein und einige Abschnitte ständig als belegt angezeigt werden. Auch eine Basisstation der ETCS-Funkübertragung kann gestört sein. Dadurch ist eine Übertragung der Fahrerlaubnis zwischen RBC und Zug im Bereich der gestörten Basisstation nicht möglich.

All diese Ereignisse haben die Gemeinsamkeit, dass es sich meistens nur um einen punktuellen Einzelausfall mit einer sehr geringen Anzahl von betroffenen Systemen oder mit einem sehr kleinen betroffenen Bereich handelt. Im Gegensatz zum begrenzten Ausmaß eines Safety-Ereignisses kann im Fall eines einzelnen IT-Angriffs aufgrund der Vernetzung eine höhere Anzahl von Systemen betroffen sein sowie die Störung eine breitere räumliche Ausdehnung haben. Meistens haben kommerzielle IT-Systeme, auch bekannt als commercial off-the-shelf systems, kurz COTS, die gleiche Einstellung bzw. Konfiguration. Ist eine Schwachstelle im COTS-System vorhanden, kann der Angreifer die Schwachstelle ausnutzen und den Angriff durch die IT-Vernetzung schnell in großem Still ausbreiten.

Wie bereits erwähnt, waren von dem Angriff des Ransomware-Schadprogramms WannaCry an einem Wochenende im Mai 2017 weltweit mindestens 200.000 Rechnersysteme in 150 Ländern betroffen, darunter auch die Fahrgastinformation, Kameras und Ticketautomaten der Deutschen Bahn [8]. Das Ausmaß eines IT-Angriffs kann jedoch sehr unterschiedlich sein. Es kann sich

je nach Motivation des Angreifers gezielt auf bestimmtes System beschränken, wie bei dem Fall Stuxnet [4] bekannt ist. Es kann sich jedoch auch, wie der Fall WannaCry, weltweit über die geografische Grenze hinaus auf hunderttausende Systeme ausbreiten. Bei einer Spiegelung auf die zukünftige Eisenbahn mit einer hohen Digitalisierung und Vernetzung kann dies nur bedeuten, dass im zukünftigen Bahnbetrieb mit häufigeren, großräumigeren sowie systemübergreifenden Störungen gerechnet werden muss. Bekannt ist, dass bereits ein einfacher Security-Angriff mittels physikalischer Gewalt ein betriebliches Chaos anrichten kann. Dies war bei dem Angriff durch gezielte Beschädigungen der Signalkabel zwischen Duisburg Hbf und Düsseldorf Flughafen im September 2018, der ein 3-tägiges Bahn-Chaos im Großraum Duisburg / Düsseldorf verursacht hat [36, 37], der Fall. Die kommende Bedrohung durch IT-Angriffe stellt daher eine große Herausforderung in einer neuen Dimension für den zukünftigen Bahnbetrieb in Rückfallebenen dar.

Nicht nur die Digitalisierung und die IT-Vernetzung haben günstigere Gegebenheiten für einen Angreifer erschaffen, ein größeres Ausmaß einer Störung oder von Ausfällen mit einem einzigen Angriff aus der Ferne anrichten zu können. Auch der Trend zur Miniaturisierung bzw. Virtualisierung des technischen Systems ist mit anderen gemeinsam dafür verantwortlich. Das heutige IT-System wird immer kompakter, komplexer und leistungstärker. Daher können mehrere Prozesse bzw. Funktionen gleichzeitig parallel in einem IT-System ausgeführt werden oder von demselben IT-System erbracht werden, die früher wegen der mangelnden Rechenleistung auf diverse physikalisch getrennte IT-Systeme aufgeteilt und separat ausgeführt werden mussten [24]. Die steigende Rechenleistung und die daraus resultierende Miniaturisierung und Virtualisierung hat dazu geführt, dass zum Beispiel auch die sicherheitsrelevanten und nicht-sicherheitsrelevanten Prozesse bzw. Funktionen, die strikt voneinander getrennt werden sollten, gemeinsam von einem IT-System ausgeführt werden können. Die erforderliche Trennung zwischen den Prozessen wird dann durch die Software virtuell realisiert. D. h.: Alle Prozesse desselben IT-Systems teilen sich im Prinzip die gleichen physikalischen Ressourcen für die Realisierung des eigenen Funktionsziels, z. B. den gleichen Arbeitsspeicher, den gleichen Prozessor sowie denselben Übertragungskanal. Dies hat zur Folge, dass mehrere prozesstechnisch unabhängige Funktionen eines technischen Systems zugleich ausfallen können, wenn das gemeinsame IT-System der Prozesse z. B. durch einen IT-Angriff gestört ist.

Diese Änderung des Ausmaßes einer Störung bezüglich der Anzahl der betroffenen Funktionen hat erhebliche Auswirkungen auf die Betriebsführung in der Rückfallebene. Während bei dem konventionellen Safety-Ereignis bisher meistens nur vom Einzelausfall die Rede ist, worauf das heutige Konzept der Betriebsführung in der Rückfallebene z. B. im Eisenbahnbereich aufbaut, muss bei der zukünftigen Gestaltung von Rückfallebenen berücksichtigt werden, dass derartige Mehrfachausfälle durch die IT-Entwicklung und die zunehmenden IT-Angriffe häufiger auftreten können.

2.2.4 Priorität

Darüber hinaus ist zu beachten, dass sich auch die Prioritäten zur Behandlung von Ereignissen mit dem gleichen Anzeichen aus Safety- und Security-Sicht widersprechen können und daher ein Kompromiss zwischen den Safety und Security gefunden werden muss. Ein häufiges Beispiel ist der Umgang mit dem Ausgang eines geschützten Gebäudes. Im Fall eines Feueralarms muss der Ausgang aus Safety-Sicht zur schnellen Evakuierung gleich offen gelassen werden, jedoch sollte er aus Security-Sicht zunächst geschlossen bleiben, damit der Angreifer, der den Alarm mit unbekannter Motivation absichtlich aktiviert hat, nicht aus dem Gebäude entkommen kann. Ein weiteres Beispiel wäre die Notfalldurchsage im Eisenbahnbetrieb: Aus Safety-Sicht (es wäre tatsächlich einen Notfall) spielen die Authentizität und die Glaubwürdigkeit der Information im Vergleich zu der Verfügbarkeit und der Rechtzeitigkeit der Information keine wichtige Rolle, da es bei einem Fehlalarm grundsätzlich nur zum sicheren Stillstand des Betriebs kommen kann. Aus IT-Security-Sicht ist jedoch wichtig, dass die Notfalldurchsage nicht absichtlich von einem Angreifer erzeugt werden kann, damit der Betrieb normal durchgeführt werden kann und nicht ständig von dem Fehlalarm beeinträchtigt wird. Diese zusätzliche Anforderung durch die IT-Security ist aber aus Safety-Sicht nicht immer erwünscht, da die Übertragung der zeitkritischen Notfalldurchsage durch die stärkeren Authentifizierungsverfahren zeitlich verzögert werden kann. D. h.: Auch wenn die Implementierung von Gegenmaßnahmen mit der Entwicklung des IT-Angriffs mithalten könnte, ist es an viele Stellen unerlässlich, eine Priorität zwischen dem Safety-Ziel und dem Security-Ziel zu setzen und einen Kompromiss zu finden bzw. einen Verlust anzunehmen. Eine hundertprozentige, absolute Sicherheit wird es nicht geben.

2.2.5 Dauer

Als letztes ist anzunehmen, dass die Dauer der Reparatur nach einem IT-Angriff bzw. die Dauer der Betriebsführung in den Rückfallebenen zukünftig ebenfalls länger dauern wird. Einerseits gibt es wegen der großen Ausdehnung eine steigende Anzahl der betroffenen Funktionen bzw. Systeme, die zwar gleichzeitig von demselben Angriff betroffen waren, die aber z. B. aus sicherheitstechnischen Gründen vereinzelt repariert und wieder abgenommen werden müssen. Dadurch kann bereits aufgrund der begrenzten Anzahl von verfügbarem Fachpersonal eine längere Dauer der Reparatur erwartet werden. Konventionell kann die Störung bei einem Safety-Ereignis durch die Reparatur durch Redundanz bzw. durch einen Austausch durch ein identisches System zügig behoben werden. Da die Ursache eines Ereignisses, ob Safety oder Security, nicht immer (rechtzeitig) zu identifizieren ist, müsste die Störung in diesen Fällen analog zu den traditionellen Störungen eines Safety-Ereignisses behandelt werden. Diese Vorgehensweise kann die Störung aber bei einem tatsächlichen IT-Angriff nicht beheben, wenn das Ersatzsystem die gleiche Schwachstelle wie das gestörte System hat. Im ungünstigsten Fall kann ein Austausch eines „identischen“ Systems das Ausmaß des Angriffs sogar weiter vergrößern. Das Ersatzsystem z. B. kann zwar die komplette identische Safety-Eigenschaft wie das gestörte System besitzen. Dieses hat jedoch nicht die gleiche Security-Eigenschaft, da das

entsprechende Update nur bei Systemen im Betrieb durchgeführt wurde. Zudem könnte es aufgrund der Komplexität des heutigen IT-Systems auch schwierig sein, bei der Behebung von Security-Ereignissen aus IT-Angriffen alle Schäden in einer Software in einer begrenzten Zeit genau zu identifizieren. Dies führt dann dazu, dass ein Teil des Schadprogramms nach der angeblich erfolgreichen Reparatur weiterhin im System geblieben ist und dieses bei der nächstgünstigen Gelegenheit wieder zum Sturz bringen könnte.

2.2.6 Zusammenfassung

Die Bedrohung durch einen IT-Angriff wird durch die rasante Entwicklung der IT und der IT-Vernetzung auch für eine Kritische Infrastruktur, wie z. B. das System Eisenbahn, immer ernster. Es ist zwar davon auszugehen, dass eine komplette Übernahme der sicherheitsrelevanten Funktionen aufgrund der Komplexität und des Designs eines modernen Eisenbahnsystems sehr unwahrscheinlich ist. Jedoch steigt die Möglichkeit, dass das System Bahn durch den IT-Angriff häufiger gestört wird und dessen Betrieb häufiger in der Rückfallebene fortgeführt werden muss. Zusätzlich weist ein IT-Angriff sowie dessen Folge in der in sich wachsenden IT und deren IT-Umgebung einen deutlich charakteristischeren Unterschied zu dem traditionellen Safety-Ereignis auf, insbesondere bei der Offenbarung, der Häufigkeit, dem Ausmaß und der Dauer des Ereignisses, wie in Tabelle 1 zusammengefasst wurde.

Tabelle 1: Vergleich von Safety-Ereignis und IT-Security-Angriff anhand beispielhafter Kriterien

Kriterien	Safety-Ereignis	IT-Security-Angriff
<i>Maßnahmen zur Offenbarung</i>	<ul style="list-style-type: none"> Sehr ausgereifte Maßnahmen vorhanden 	<ul style="list-style-type: none"> Noch in der Anfangsphase. Die Bedrohung ist dem Stand der Technik häufig einen Schritt voraus
<i>Dauer zur Offenbarung</i>	<ul style="list-style-type: none"> Generell schnell, da es mit den ausgereiften Maßnahmen zügig erkennbar ist. 	<ul style="list-style-type: none"> Kann bis zu Monaten dauern, da es schwierig ist, die Ursache in kurzer Zeit zu identifizieren bzw. von einem Safety-Ereignis zu unterscheiden
<i>Häufigkeit des Ereignisses</i>	<ul style="list-style-type: none"> Einschätzbar und meist statistisch belegbar, da die Umgebung quasi stabil ist. 	<ul style="list-style-type: none"> Nicht einschätzbar, da die Umgebung dynamisch ist. Außerdem ist der Angriff von z. B. der Motivation, Fähigkeit und Ressourcen des Angreifers abhängig.
<i>Anzahl des Systems</i>	<ul style="list-style-type: none"> Einzelsystem oder nur sehr geringe Anzahl von Systemen 	<ul style="list-style-type: none"> Kann sehr viel sein, da die Systeme miteinander verbunden sind
<i>Räumliche Ausdehnung</i>	<ul style="list-style-type: none"> Meist nur punktuell oder ein kleiner Bereich 	<ul style="list-style-type: none"> Kann sehr großräumig sein, da die geografische Grenze wegen der IT-Vernetzung wegfällt
<i>Anzahl der Funktion</i>	<ul style="list-style-type: none"> Meist nur eine oder nur sehr geringe Anzahl von Funktionen 	<ul style="list-style-type: none"> Kann aufgrund der Virtualisierung sehr viel sein
<i>Dauer der Reparatur</i>	<ul style="list-style-type: none"> Meist sehr schnell, da es durch die Redundanz oder den Austausch von Ersatzteil direkt zu lösen ist 	<ul style="list-style-type: none"> Kann sehr lange dauern, da es durch eine Redundanz oder den Austausch von Ersatzteilen nicht direkt gelöst werden kann

D. h., dass der zukünftige Eisenbahnbetrieb unter der Bedrohung durch einen IT-Angriff voraussichtlich nicht nur häufig in der Rückfallebene geführt werden muss, sondern auch häufiger mit Mehrfachausfällen von Funktionen bzw. Systemen sowie großräumigen Störungen in den Rückfallebenen konfrontiert wird. Letztendlich trägt die Rückfallebene die wesentliche Verantwortung für die Aufrechterhaltung der Funktionalität der Bahn nach einem IT-Angriff. Daher wird das Rückfallebenenkonzept des Bahnbetriebs in dem nächsten Kapitel eingehend behandelt.

2.3 Bahnbetrieb und dessen Rückfallebenenkonzept

2.3.1 Bestandteile des Bahnsystems und dessen Aufgaben

Seit Anfang der Bahn-Geschichte hat das System Bahn als Verkehrsmittel die Aufgabe, Personen und Güter zu transportieren. Diese elementare Aufgabe der Bahn hat sich bis heute nur unwesentlich verändert. Um die grundlegende Transportaufgabe der Bahn realisieren zu können, benötigt die Bahn so wie auch alle anderen Verkehrsmittel ein bestimmtes „Transportgefäß“, z. B. das Fahrzeug bei der Bahn und das Flugzeug in der Luftfahrt, in dem die Menschen oder Güter untergebracht und dann als eine Transporteinheit befördert werden können. Anders als die Luftfahrt, die für ihre Flugbewegung im Himmel keine zusätzliche bauliche Infrastruktur benötigt, ist die bauliche Infrastruktur für den Betrieb der Bahn jedoch unverzichtbar. Als spurgeführtes Verkehrssystem benötigt die Bahn eine elementare bauliche Infrastruktur, um das Fahrzeug während des Betriebs zu tragen sowie dessen Bewegung zu führen [38]. Die für die Fahrzeugbewegung erforderlichen Antriebs- und Bremskräfte werden bei den meisten Bahnen durch das Fahrzeug erzeugt. Diese können jedoch auch von der Infrastruktur bereitgestellt werden, wie es bei der Zahnradbahn und der Magnetschwebbahn der Fall ist. So kann der Zweck des Bahnbetriebs wie in [39] allgemein beschrieben werden: *„Zweck des Bahnbetriebs ist die Durchführung von Fahrten mit Eisenbahnfahrzeugen auf einer Eisenbahninfrastruktur“*.

Um jedoch bei der Durchführung von Fahrten eine bestimmte Betriebsqualität erreichen zu können, ist neben dem Fahrzeug und der Infrastruktur ein System betrieblicher Regeln unerlässlich. Die betrieblichen Regeln haben vor allem die Aufgaben, die vorgesehene Betriebsqualität des Bahnbetriebs „fiktiv“ zu realisieren und zu gewährleisten. Sie enthalten z. B. die Regeln der Funktionssteuerung, die Logik der Steuerprozesse sowie die Beschreibung der Prozessabläufe. Daher sind die betrieblichen Regeln des Bahnbetriebs nach [39] durchaus mit der „Software“ eines Rechensystems vergleichbar. Die Software eines Rechensystems allein ist nicht mehr als eine Menge von Zeichen, die einer bestimmten Logik unterliegen. Auch die Hardware eines Rechensystems allein ist nicht mehr als eine Menge von festen Gegenständen, die bestimmte physikalische Eigenschaften und Fähigkeiten besitzen, aber keine Logik zur Realisierung der Systemfunktion enthalten.

D. h., um die vorgesehenen Systemfunktionen eines Rechensystems zu realisieren, benötigt das Rechensystem eine Software, welche die zusammenhängende Nutzung der verschiedenen Hardwares bzw. Teilsysteme regelt bzw. steuert. Zugleich benötigt das Rechensystem aber auch die geeigneten Hardwares, welche die Ausführung der Software bzw. die Realisierung der Systemfunktion zu tragen haben. Darüber hinaus kann ein Rechensystem je nach dessen Zweck sowie Automatisierungsgraden die aktive Teilnahme von Menschen als System-Bediener in dessen Prozessen einbeziehen oder nicht. So besteht ein funktionierendes Rechensystem aus der Software und der geeigneten Hardware mit oder ohne Menschen als System-Bediener. Eine Übertragung dieses Konzepts auf das Eisenbahnsystem bedeutet, dass ein funktionierendes

Eisenbahnsystem nicht allein aus einer Hardware, wie Fahrzeug und baulicher Infrastruktur, bestehen kann. Ohne die entsprechenden betrieblichen Regeln sowie die Bediener ist das Eisenbahnsystem unvollständig und unzweckmäßig. Vorstellbar ist ein primitives Eisenbahnsystem nach [38], in dem der Hardware-Teil lediglich aus Fahrzeug, baulicher Infrastruktur und den Menschen als die alleinigen System-Bediener und der Software-Teil allein aus betrieblichen Regeln besteht.

Die Entwicklung der Technik hat dazu beigetragen, dass heute weltweit eine Vielzahl von Eisenbahnsystemen existiert, deren Systemauslegungen deutlich voneinander zu unterscheiden sind. Mit den Fortschritten der technischen Entwicklung sowie dem Trend der Automatisierung, Digitalisierung und Autonomisierung werden die Tätigkeiten der Menschen als System-Bediener mehr und mehr durch technische Mittel unterstützt oder schließlich durch diese ersetzt. Die Menschen haben heute oft im normalen automatisierten Betriebsablauf lediglich eine passive Überwachungsfunktion. Eine aktive Teilnahme an dem Betriebsablauf ist meistens nur noch in Fällen nötig, in denen z. B. eine Störung aufgetreten ist, die sich nicht automatisch durch die Technik lösen lässt. Die hier genannten Tätigkeiten umfassen z. B. die Gewährleistung der Sicherung, Steuerung und Überwachung von Fahrten mit einem Eisenbahnfahrzeug auf der Eisenbahninfrastruktur sowie die optimale Ablaufsteuerung von Prozessen zur Abwicklung der Betriebsführung, wie die dispositive Tätigkeit [40–42].

Es ist jedoch stets anzunehmen, dass die Menschen in der Zukunft weiterhin ein wichtiger Bestandteil des Eisenbahnsystems bleiben werden. Zwar nicht in dem normalen automatisierten bzw. autonomen Betrieb, aber stets in den vielseitigen Störungsszenarios. Wird das Eisenbahnsystem in seiner Gesamtheit betrachtet, können die Bestandteile des modernen Eisenbahnsystems wie in Abbildung 5 schematisch dargestellt werden.

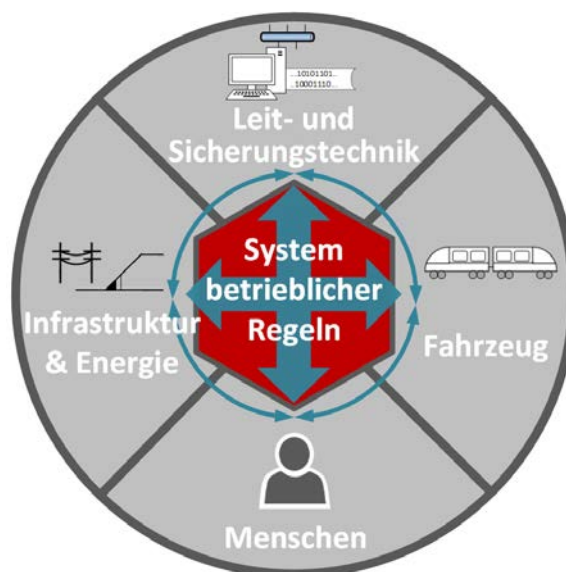


Abbildung 5: Bestandteile eines modernen Eisenbahnsystems

Im Laufe der Strukturentwicklung hat das System Bahn jedoch weitere Aufgaben bzw. Verpflichtungen auf sich genommen. Mit der Entwicklung der Infrastruktur von einer einzelnen Verbindungslinie bis zur heutigen flächendeckenden Netzstruktur hat sich das System Bahn in Deutschland als die Grundinfrastruktur zur Erfüllung des Grundbedürfnisses der Menschen auf die Mobilität sowie zur Gewährleistung der Stabilität der Gesellschaft etabliert. Durch das Inkrafttreten des Regionalisierungsgesetzes im Dezember 1993 hat das System Bahn im Bereich Personennahverkehr eine neue öffentliche Verpflichtung erhalten. Der §1 (1) des Regionalisierungsgesetzes sieht die Sicherstellung einer ausreichenden Bedienung der Bevölkerung mit Verkehrsleistungen im öffentlichen Personennahverkehr als eine Aufgabe der Daseinsvorsorge [43]. Anschließend wird die Finanzierung für den Personennahverkehr durch den staatlichen Zuschuss aus den Steuereinnahmen des Bundes, die auch als „Regionalisierungsmittel“ bekannt sind, seit 1996 bis heute gesichert.

Unter der Zusammenwirkung der gesetzlichen Anforderung und der gesicherten Finanzierung gab es von 1996 bis 2013 im Schienenpersonennahverkehr einen signifikanten Zuwachs von Fahrgastzahlen um mehr als 60%. Damit wurde die Aufgabe der Daseinsvorsorge von Mobilität erfolgreich erfüllt [44]. Heute im Jahr 2017 hat das öffentliche Schienenverkehrsnetz in Deutschland im Bereich der DB Netz AG eine gesamte Gleislänge von 60.524 km [45]. Im Bereich des Schienenpersonenverkehrs reisten im Jahr 2017 täglich über 5,68 Mio. Fahrgäste in den Zügen der DB-Gruppe, davon 0,39 Mio. im Schienenpersonenfernverkehr (SPFV) und 5,29 Mio. im Schienenpersonennahverkehr (SPNV) [46]. Auch im Bereich Güterverkehr wurden im Jahr 2017 täglich 0,95 Mio. Tonnen Güter im öffentlichen Schienengüterverkehr transportiert, was nach einer Hochrechnung mit den zurückgelegten Kilometern (Tonnenkilometern) einen Marktanteil der Verkehrsträger von ca. 17% im gesamten Güterverkehr umfasst [47].

Nach Definition der EU-Richtlinie 2008/114/EG ist ein System oder ein Teil eines Systems, welches von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung ist und deren Störung oder Zerstörung erhebliche Auswirkungen hätte, eine Kritische Infrastruktur (KRITIS) [48]. Durch die starke Einbindung in die alltäglichen Aktivitäten der Gesellschaft und die enge Verzahnung mit der industriellen Produktion und der Wirtschaft spielt das heutige System Bahn in Deutschland neben ihrer elementaren Transportaufgabe zugleich eine bedeutende Rolle für das Funktionieren und den Stabilitätsverlust der Gesellschaft und der Volkswirtschaft. Das Nicht-Funktionieren des heutigen Eisenbahnsystems kann auf Dauer eine schwerwiegende negative Auswirkung zur Folge haben und im ungünstigen Fall zum Kollaps der Gesellschaft und der Wirtschaft führen. Damit fallen große Eisenbahnverkehrsunternehmen (EVU) sowie Eisenbahninfrastrukturunternehmen (EIU) in Deutschland in die Kategorie der Kritischen Infrastrukturen, an die besondere Anforderungen gestellt werden.

Die Anforderung, Maßnahmen zum Erhalt der Funktionsfähigkeit eines Unternehmens zu treffen, ist nicht neu. Aktiengesellschaften und große Gesellschaften mit beschränkter Haftung

werden durch Aktiengesetz Paragraph § 91 aufgefordert, Maßnahmen zu treffen, damit den Fortbestand der Unternehmen gefährdende Entwicklungen frühzeitig erkannt und ihnen entgegengewirkt werden kann [49]. Das bedeutet, dass sich, je nach Art der Kritischen Infrastrukturen, die Betreiber der Bahn bereits heute auf erhebliche, das Gemeinwesen beeinflussende Ereignisse, die durch Naturereignisse, technisches und / oder menschliches Versagen, vorsätzliche Handlungen mit terroristischem oder sonstigem kriminellen Hintergrund sowie Krieg ausgelöst werden können, vorbereiten müssen.



Abbildung 6: Elementare Aufgaben der Bahn

Mit dem IT-Sicherheitsgesetz von Juli 2015 müssen Kritische Infrastrukturen wie das Bahnsystem außerdem erweiterten Vorgaben genügen, in welchen die entsprechenden Maßnahmen zur Aufrechterhaltung ihrer IT-Systeme, die für die Funktionsfähigkeit der Kritischen Infrastruktur maßgeblich sind, gefordert werden. Die gesetzlichen Vorgaben referenzieren vor allem die geforderte Funktionsfähigkeit der Systeme bzw. der Kritischen Infrastruktur, ohne auf weitergehende Qualitätsaspekte, wie beispielsweise Sicherheit, einzugehen. Das System Eisenbahn ist zwar eine Kritische Infrastruktur mit volkswirtschaftlicher Bedeutung und trägt dazu bei, dass das Grundbedürfnis der Menschen auf Mobilität erfüllt und Funktionen sowie die Stabilität der Gesellschaft aufrechterhalten werden können, wie in Abbildung 6 dargestellt ist. Es ist aber zu beachten, dass das System Eisenbahn nicht das einzige Transportmittel ist, das die benannten elementaren Aufgaben erfüllen kann. Um die Rolle der Bahn im Wettbewerb der Verkehrsmittel verteidigen zu können, was auch als Teil der Aufrechterhaltung ihrer Funktionsfähigkeit angesehen werden kann, müssen die Qualitätsvorteile der Bahn gegenüber den anderen Verkehrsmitteln vorerst hervorgehoben werden.

2.3.2 Qualitätsmerkmale des Bahnbetriebs

Im Qualitätsvergleich zwischen den motorisierten Verkehrsmitteln im Landverkehr zeigt die Bahn ihre Stärke bzw. Vorteile im Thema Transport-Sicherheit und Transport-Leistung. Sowohl in Deutschland als auch überall in Europa gilt die Bahn als das sicherste Verkehrsmittel im Landverkehr. Die hohe Sicherheit der Bahn gegenüber den anderen Verkehrsmitteln war und bleibt die ausschlaggebende Stärke der Bahn. Wie in der EU-Richtlinie 2016/798

Eisenbahnsicherheit beschrieben wurde, verfügt das Eisenbahnsystem in Europa generell über ein hohes Sicherheitsniveau, insbesondere im Vergleich zum Straßenverkehr [50].

Statistisch gesehen ist die Anzahl der getöteten bzw. verletzten Reisenden pro Milliarde Personenkilometer für Insassen eines Pkw in Deutschland von 2007 bis 2016 im Durchschnitt 53-mal bzw. 125-mal höher als für Bahnreisende. Auch im Bereich Gütertransport ist die Wahrscheinlichkeit der Gefahrgutunfälle auf der Straße pro Milliarde Tonnenkilometer von 2004 bis 2013 im Durchschnitt 42-mal höher als auf der Schiene [51]. Im Thema Transportleistung hat die Bahn die anderen Verkehrsmittel ebenfalls stets überwiegend geschlagen. Egal, ob im Personenverkehr oder im Güterverkehr: Die Bahn hat eine deutlich größere Beförderungskapazität pro Transporteinheit im Vergleich zu den anderen Verkehrsmitteln. Z. B. kann eine 150 Meter lange S-Bahn so viele Personen befördern wie 436 Pkw mit einem durchschnittlichen Pkw-Besetzungsgrad von 1,2 Personen im Berufsverkehr. Auch im Containerverkehr kann ein einlagiger 740-Meter-Güterzug mit 35 Waggons die Transportmenge von 52 Lkw ersetzen [52–56].

Das Entscheidende ist jedoch, dass die Bahn trotz ihrer großen Beförderungsmengen ihre Transportaufgabe weiterhin mit sehr hoher Geschwindigkeit und einer dichten Zugfolge realisieren kann. Mit der modernen Technik ist heutzutage eine Mindestzugfolgezeit von 3 Minuten im SPFV bei einer Geschwindigkeit bis zum 350 km/h [57, 58] bzw. 1,5 Minuten im SPNV [59–61] bei vielen Bahnen als Standardanforderung möglich. Auch auf einer Strecke mit Mischverkehr von Güterzügen und Personenzügen lässt sich in Deutschland seit Jahren eine dichte Zugfolgezeit von 4 Minuten durch eine vollständige Harmonisierung der Geschwindigkeiten aller Züge erreichen. Als Beispiele sind die engen Taktungen auf den Streckenabschnitten Hamburg-Hannover, Offenburg-Basel und Minden-Wunstorf zu sehen [62].

D. h., die Funktion der Bahn unterscheidet sich von den anderen Verkehrsmitteln, indem sie eine deutlich größere Anzahl bzw. Menge von Reisenden bzw. Gütern in demselben Zeitraum und außerdem schneller und sicherer befördern kann. Allerdings reichen die hohe Sicherheit und das große Leistungsniveau allein nicht aus, um alle Aufgaben der Bahn zu realisieren. Die Bahn als Kritische Infrastruktur hat, wie oben beschrieben, die Aufgabe, ihre Funktionen in der Gesellschaft aufrechtzuerhalten. D. h., das erwartete Leistungsniveau der Bahn darf nicht nur als Spitzenwert erscheinen, sondern muss auch über einen längeren Zeitraum möglichst konstant und verlässlich verfügbar sein. Bei dem System Bahn können daher drei ausschlaggebende Qualitätsmerkmale identifiziert werden, die sich wesentlich von den anderen Verkehrsmitteln im Landverkehr unterscheiden. Die sind, wie die Abbildung 7 darstellt, die hohe Sicherheit, ein großes Leistungsniveau und die hohe Verfügbarkeit. Das Konzept der Verfügbarkeit setzt sich nach DIN EN 50126-1 aus Zuverlässigkeit, Instandhaltbarkeit, Instandhaltung und Betrieb des Systems zusammen [27]. Während sich die Zuverlässigkeit, Instandhaltbarkeit und Instandhaltung z. B. mit den Ausfallarten, -raten, Auswirkungen sowie den Reparaturen auseinandersetzen, beschäftigt sich der Betrieb sowohl im normalen Bahnbetrieb als auch in der Rückfallebene mit dem Konzept der Betriebsfortführung. Die

Rückfallebene des Bahnbetriebs kann daher funktional als eine alternative Ausführungsvariante des Bahnbetriebs verstanden werden, die dazu dient, die vorgesehene Betriebsqualität trotz des Einflusses eines bestimmten Ereignisses möglichst weiter zu erbringen.

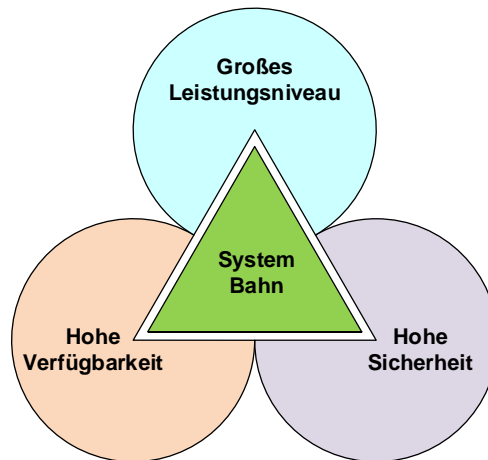


Abbildung 7: Ausschlaggebende Qualitätsmerkmale des Bahnsystems

Die Anforderung auf ein leistungsfähiges und verfügbares Bahnsystem ist nicht neu. In der EU-Richtlinie 2012/34/EU wurde bereits gefordert, dass den EVU und EIU Anreize zur Minimierung von Störungen bzw. zur Erhöhung der Verfügbarkeit sowie zur Erhöhung der Leistungsfähigkeit geboten werden [63]. Das Ziel, ein leistungsfähiges, sicheres und zugleich hoch verfügbares Konzept der Betriebsführung zu erstellen, ist eine Herausforderung. Es fordert eine sorgfältige Überlegung des Betreibers sowie die Abstimmung und den Kompromiss der Akzeptanz der Gesellschaft bzw. der Politik. Ungeachtet der wirtschaftlichen Kosten eines Betriebskonzepts, kann z. B. ein Betriebskonzept mit einem zu hohen Anspruch auf die Sicherheit dessen Leistung und Verfügbarkeit massiv einschränken. Doch auch ein Betriebskonzept mit einem ungleichen Fokus auf die Leistung kann dessen Sicherheit und Verfügbarkeit ebenfalls erheblich gefährden.

2.3.3 Die rechtliche Forderung auf die Rückfallebene des Bahnbetriebs

Die Forderung auf das Rückfallebenenkonzept ist z. B. bei dem Teilsystem Sicherungstechnik auf EU-Ebene rechtlich in der Richtlinie EU 2016/797 über die Interoperabilität des Eisenbahnsystems in der Europäischen Union verankert. In Bezug auf die Sicherungstechnik wird im Anhang III, Abschnitt 2.3.1 der Richtlinie wie folgt vorgeschrieben: *„Die Anlagen und Verfahren der Zugsteuerung/Zugsicherung und Signalgebung müssen einen Zugverkehr entsprechend den Sicherheitsvorgaben für das Netz ermöglichen. Die Zugsteuerungs-/Zugsicherungs- und Signalgebungssysteme müssen weiterhin den sicheren Verkehr von Zügen ermöglichen, deren Weiterfahrt unter vorgegebenen Einschränkungen gestattet ist.“* [41] Die in dem letzten Satz beschriebene *„Weiterfahrt unter vorgegebenen Einschränkungen“* deutet darauf hin, dass es Rückfallebenen in der Sicherungstechnik geben muss, damit der Bahnbetrieb unter gewissen Einschränkungen trotzdem weiter stattfinden kann. Zum Beispiel kann es während des automatisierten Betriebsablaufs vorkommen, dass die Zulassung einer Zugfahrt,

die normalerweise automatisch durch eine Fahrstellung des Signals erfolgen sollte, wegen einer Signalstörung nicht mehr automatisch ausgeführt werden kann. Dazu kann der Fahrdienstleiter (Fdl) als Rückfallebene z. B. den Triebfahrzeugführer (Tf) per Funk kontaktieren und die Zulassung der Zugfahrt per Befehl an den Tf erteilen. So wird der Begriff Rückfallebene im Bereich Sicherungstechnik nach [64] als *„durch den Bediener gebildeter Ersatzkanal für den Fall, dass eine Komponente der Sicherungsanlage ausgefallen ist“* spezifiziert.

Nicht nur im Bereich Sicherungstechnik, sondern auch an den gesamten Betrieb wird die Forderung auf ein Rückfallebenenkonzept im Anhang II, Abschnitt 2.5 der Richtlinie unter *„Betriebsführung und Verkehrssteuerung“* gestellt. Dort werden die Anforderung wie folgt beschrieben: *„Verfahren und zugehörige Ausrüstungen, die eine kohärente Nutzung der verschiedenen strukturellen Teilsysteme erlauben, und zwar sowohl im Normalbetrieb als auch bei Betriebsstörungen, einschließlich insbesondere der Zugbildung und Zugfahrten, der Planung und der Abwicklung der Betriebsführung.“* [41] Diesbezüglich muss es daher auch teilsystemübergreifende Rückfallebenen geben, welche die Durchführung des Bahnbetriebs bei der Betriebsstörung in Allgemeinen ermöglichen.

Die beiden oben benannten Forderungen auf das Rückfallebenenkonzept sind allgemein an das gesamte Eisenbahnsystem bzw. den gesamten Eisenbahnbetrieb gerichtet, ohne eine Differenzierung der Verantwortung zwischen EVU und EIU. Anders als EVU, deren Hauptaufgabe in der Beförderung von Gütern und / oder Personen besteht, wodurch die Funktionalität des Teilsystems Fahrzeug sichergestellt werden muss, haben EIU als Infrastrukturbetreiber die Verantwortung über die Funktionalität der baulichen Infrastruktur einschließlich der Leitung und Sicherung / Steuerung von Fahrten auf der eigenen Netzinfrastuktur [63]. D. h., ein EIU hat die Aufgabe, einen Überblick über die gesamte Betriebsabwicklung im Netz zu schaffen und diese qualitätsgemäß zu steuern. Rechtlich ist in der Richtlinie 2012/34/EU Artikel §53 geregelt: *„Bei technisch bedingten oder unfallbedingten Störungen der Zugbewegungen hat der Infrastrukturbetreiber alle erforderlichen Maßnahmen zu treffen, um die Situation wieder zu normalisieren“*. Somit erhält das EIU dadurch auch die entscheidende Rolle der Durchführung von Rückfallebenenkonzepten.

Das bedeutet, dass der gesamte Aspekt des Rückfallebenenkonzepts den rechtlichen Anforderungen zufolge sowohl einzelne und kleinräumige Störungen eines Teilsystems als auch mehrfache und großräumige Betriebsstörungen abdecken muss. Darüber hinaus müssen EIU ihre *„Regeln für den Umgang mit größeren Betriebsstörungen und Notfällen“* gemäß Anhang V der Richtlinie vertraglich mit den zuständigen Behörden vereinbaren [63]. Die leitende Aufgabe im Bahnbetrieb liegt dann in der Verantwortung des Infrastrukturbetreibers, wie in der Richtlinie 2016/798 Eisenbahnsicherheit vorgeschrieben ist: *„(32) Die Infrastrukturbetreiber sollten eine zentrale Verantwortung für die Sicherheit der Planung, der Instandhaltung und des Betriebs ihres Eisenbahnnetzes haben. [...]“* [50] Sicherlich haben die Verantwortung zur Sicherstellung der Betriebsqualität sowohl EIU als auch EVU zu tragen und bei der Durchführung von Rückfallebenen zusammenzuarbeiten [50, 65]. Trotzdem haben EIU als Infrastrukturbetreiber die Oberhand bei der Gestaltung und Umsetzung des

Rückfallebenenkonzepts im Hinblick auf den gesamten Bahnbetrieb. Demzufolge wird für diese Arbeit die Annahme getroffen, dass die Analyse der Rückfallebene in den anschließenden Kapiteln vornehmlich aus Sicht des Infrastrukturbetreibers betrachtet wird.

2.3.4 Der Übergangsprozess zwischen dem Normalbetrieb und der Rückfallebene¹

Das Konzept des Bahnbetriebs im normalen Systemzustand und das Konzept der Betriebsfortführung in der Rückfallebene bilden zusammen ein komplettes „Konzept der Betriebsführung“ für das System Bahn, deren Übergänge im heutigen Bahnbetrieb meistens durch einen definierten und geregelten Übergangsprozess eingebunden sind. Wie die Abbildung 8 darstellt, besteht der Übergangsprozess des Bahnbetriebs aus vier Prozessphasen:

- Phase 1: Regelbetrieb,
- Phase 2: Übergangsphase vom Regel- in den Störungsbetrieb
- Phase 3: Störungsbetrieb,
- Phase 4: Übergangsphase vom Störungsbetrieb zurück in den Regelbetrieb

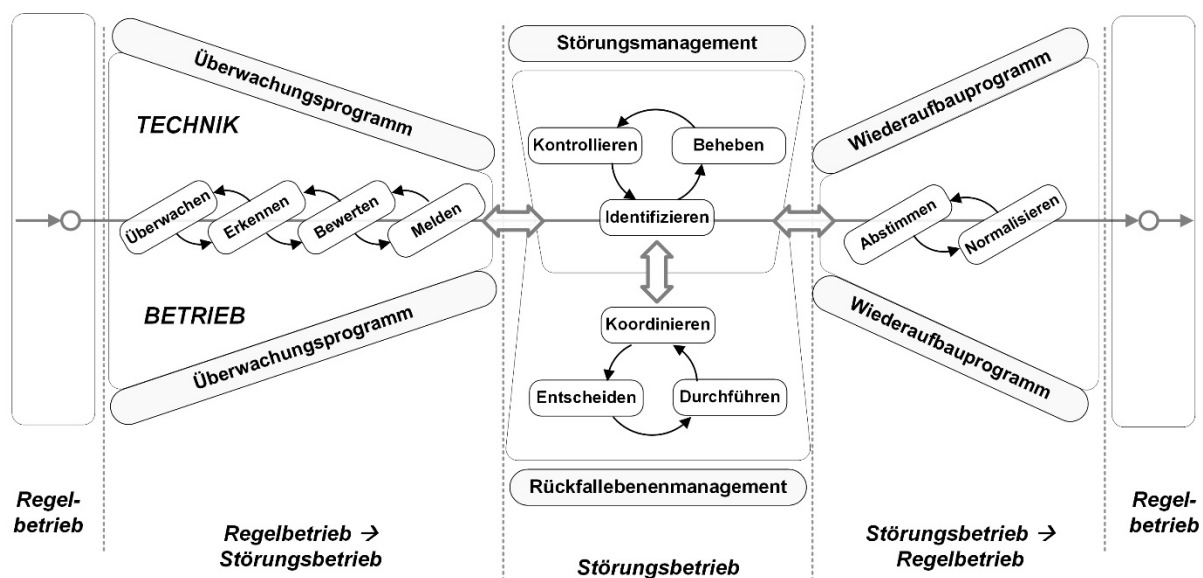


Abbildung 8: Bestehender Systemprozessablauf im Bahnbetrieb [1]

Die Aktivitäten während der Phasenentwicklung können allgemein in vier Programmabläufe spezifiziert werden: Überwachungsprogramm, Störungsmanagement, Rückfallebenenmanagement und Wiederaufbauprogramm. Außerdem lässt sich der Aspekt der Betrachtung weiter nach „Technik“ und „Betrieb“ aufteilen. In jeder Phase finden definierte Programme bzw. Aktivitäten statt:

- Überwachungsprogramm
 - Das Überwachungsprogramm besteht aus den Aktivitäten Überwachen, Erkennen, Bewerten und Melden. Im heutigen modernen System wird das Überwachungsprogramm

¹ Dieser Abschnitt beruht zum Teil auf der autoreigenen Veröffentlichung in [1]

sowohl durch die Technik als auch durch den Betrieb realisiert. Beispielsweise kann die Technik eine regelmäßige und automatisierte Kontrolle über eine bestimmte Funktion liefern. Ist eine Störung oder Unregelmäßigkeit aufgetreten und wird diese durch die Technik erkannt, wird eine entsprechende Prozesskette zur weiteren Behandlung angestoßen. Auch das betriebliche Personal überwacht im Rahmen der Betriebsabwicklung den Betrieb und beobachtet dessen Verlauf. Wird eine Unregelmäßigkeit entdeckt, muss das betriebliche Personal beispielsweise das von ihm beobachtete Ereignis regelwerkkonform an die zuständige Stelle melden und entsprechende Prozesse zur Minimierung der betrieblichen Auswirkungen einleiten.

- **Störungs- und Rückfallebenenmanagement**

Ist eine Meldung über eine Unregelmäßigkeit oder Störung bei der zuständigen Stelle eingegangen, muss die Art der Meldung sowie deren Ursache technisch und betrieblich identifiziert werden. Ist eine direkte bzw. umgehende Behebung der Störung nicht durchführbar, muss zur Fortführung des Betriebs die entsprechende Rückfallebene eingeführt werden. Parallel zum Betrieb in der Rückfallebene werden auf der technischen Seite die Behebungsarbeiten ausgeführt. Störungs- und Rückfallebenenmanagement stehen in engem Austausch. Insbesondere bei der Identifizierung der Störung oder der Unregelmäßigkeit und deren Ursache kann zum Beispiel die Kenntnis über die betrieblichen Abläufe für die Aufklärung der Ursache benötigt werden.

- **Wiederaufbauprogramm**

Wurde die Störung oder Unregelmäßigkeit behoben und die Funktionalität technisch kontrolliert, folgt anschließend eine Abstimmung zwischen dem Störungs- und dem Rückfallebenenmanagement, um die vorher gestörte Funktion wieder in den laufenden Betrieb einzubringen. Durch den heute modularisierten Systemaufbau und die daraus entstandene Möglichkeit, Teilfunktionen getrennt zu bedienen, ist auch ein stufenweiser Wiederaufbau möglich.

Der Aufgabenbereich des Rückfallebenenkonzepts entspricht überwiegend den Aktivitäten in der Phase Störungsbetrieb. D. h., die Aktivitäten der Überwachung bzw. die Maßnahmen der Offenbarung von Ereignissen werden im Rahmen dieser Arbeit nicht als Aufgabenbereich der Rückfallebene betrachtet. Die Rückfallebene hat, wie definiert, lediglich den Fokus, den Betrieb unter dem Einfluss eines bestimmten Ereignisses qualitätsgemäß fortzuführen. Es wird daher vorausgesetzt, dass das Ereignis, welches zur Anwendung einer bestimmten Rückfallebene führen sollte, durch die technische Maßnahme oder einen betrieblichen Ablauf im Überwachungsprogramm offenbart wird. Dadurch beginnt der Aufgabenbereich der Rückfallebene erst nach der Bekanntgabe des Ereignisses bzw. nach Vollenden der Aktivität „Melden“ im Überwachungsprogramm und endet bei der Aktivität „Abstimmen“ im Wiederaufbauprogramm.

2.3.5 Die Tätigkeitsfelder des Rückfallebenenkonzepts im Bahnbetrieb

Da die Abwicklungen von Fahrten im Bahnbetrieb bei den meisten Bahnen an den vorgegebenen Fahrplan gebunden sind, führen alle Ereignisse, die die Betriebsabwicklung negativ beeinflussen, zur Abweichung vom Fahrplan und zur Beeinträchtigung der Betriebsqualität [66]. Um die Betriebsqualität in der Rückfallebene möglichst aufrechtzuerhalten und die Betriebsdauer in der Störungsphase so kurz wie möglich halten zu können, spielen die Gestaltung des Rückfallebenenkonzepts und eine koordinierte Ausführung von dessen Tätigkeiten eine entscheidende Rolle. Die Tätigkeiten im Rückfallebenenkonzept lassen sich in sechs Tätigkeitsgruppen (Planen, Disponieren, Durchführen, Sichern, Behandeln und Identifizieren) bzw. in drei Tätigkeitsfelder (Betriebsleitung, Betriebsführung und Ereignisbehandlung) spezifizieren, wie die Abbildung 9 zeigt. Außerdem lassen sich die Tätigkeiten mit den Qualitätsmerkmalen des Bahnsystems in Abbildung 7 treffend zuordnen. Die grafische Darstellung in Abbildung 9 ist eine Detaillierung bzw. Systematisierung der Tätigkeiten im Störungsbetrieb, die die Tätigkeiten in den Programmabläufen in Abbildung 8, nämlich Störungsmanagement und Rückfallebenenmanagement, umfasst. Da der Fokus der Arbeit auf dem Betrieb liegt, wird das Rückfallebenenmanagement hier nach den betrieblichen Aufgaben weiter in die vier Tätigkeitsfelder Sichern, Durchführen, Planen, Disponieren konkretisiert, während das Störungsmanagement zusammengefasst vereinfacht mit Identifizieren und Behandeln dargestellt wird.

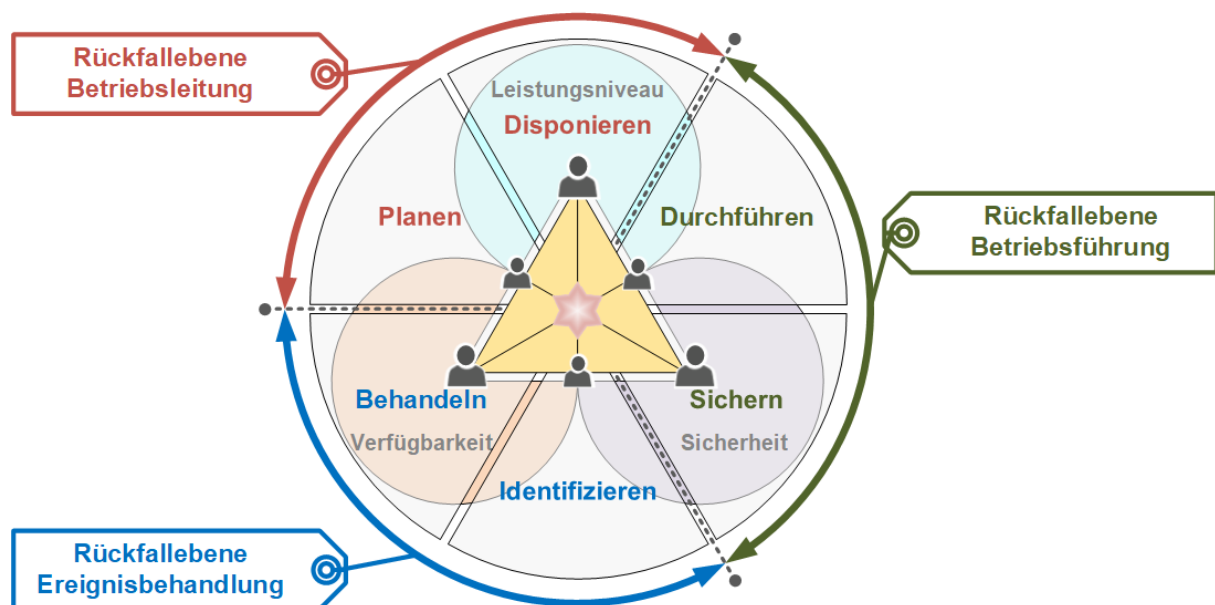


Abbildung 9: Tätigkeitsfelder des Rückfallebenenkonzepts

2.3.5.1 Tätigkeitsfeld Betriebsleitung

Das Tätigkeitsfeld Betriebsleitung hat vor allem die Aufgabe, die Fahrten in der Störungsphase umzuplanen und zu disponieren. Die Aufgabe ist ein Optimierungsvorgang des Leistungsniveaus unter den aktuellen Gegebenheiten der Betriebsabwicklung und des

Störungseinflusses. Zwar wird der Betrieb während einer Störung einige Zeit auch ohne den Eingriff der Betriebsleitung weiterlaufen können, jedoch ist das daraus resultierende Leistungsniveau in der Rückfallebene nicht immer annehmbar. Wegen der fehlenden Dispositionsmaßnahmen im Fall einer größeren Störung können z. B. alle Gleise im Bahnhof nach einer gewissen Zeit belegt sein. Da keine Züge starten und enden können, kommt es zu einer unendlichen Warteschlange im Netz, die von allein ohne den Eingriff der Betriebsleitung nicht mehr gelöst werden kann. Die Tätigkeiten der Planung und der Disposition sollen keinen direkten Einfluss auf die Sicherung der Fahrten und deren Ausführung haben. Daher haben alle Tätigkeiten der Betriebsleitung in der Regel nur das Ziel, in der Störungsphase möglichst ein kundenorientiertes Angebotsniveau und ein wirtschaftlich gerechtfertigtes Leistungsniveau des Bahnbetriebs zu erzielen. Z. B. wird in der Richtlinie 420.0101 Betriebsleitstellen der DB Netz AG wie folgt beschrieben: „§1 (2): *Die Betriebsleitstellen richten ihr Handeln auf die Wünsche aller Kunden unter Berücksichtigung der Fahrplanvorgaben und der wirtschaftlichen Zielstellung der DB-Netz AG aus. [...]*“ sowie in der 420.1000 §1 (1) „*Bei Ereignissen mit darauf zurückzuführenden massiven, netzübergreifenden Störungen im Eisenbahnverkehr gilt für den Betriebsführer und für alle beteiligten Geschäftsfelder und Eisenbahnverkehrsunternehmen: Vorrang bei allen Entscheidungen haben die Maßnahmen, die notwendig sind, um den Eisenbahnverkehr weiterzuführen.*“[67]

2.3.5.2 Tätigkeitsfeld Betriebsführung

Das zweite Tätigkeitsfeld, welches auch das maßgebliche Tätigkeitsfeld eines Rückfallebenenkonzepts ist, ist die Betriebsführung. Die Betriebsführung hat vor allem die Aufgabe, die Fahrten in der Störungsphase durch die verfügbaren alternativen Betriebsverfahren zu sichern und fortzuführen. Anders als bei der Betriebsleitung sind die Handlungen im Tätigkeitsfeld der Betriebsführung in der Regel sicherheitsrelevant. Falsche Handlungen in der Störungsphase können sofort zum Unfall führen. Besonders anfällig sind Handlungen unter menschlicher Verantwortung. Neben der Sicherheit hat die Betriebsführung auch die Aufgabe, die Fahrten qualitätsgemäß der Leistungsvorgabe aus der Planung und der Disposition der Betriebsleitung zu erbringen. Unterschiedliche Vorgaben in Deutschland zeigen jedoch unterschiedliche Aspekte zum Thema Betriebsqualität in der Betriebsführung. So heißt es im Allgemeinen Eisenbahngesetz (AEG) §4 (3) 1: „*Die Eisenbahnen [...] sind verpflichtet, ihren Betrieb sicher zu führen*“ [65]. Während das AEG lediglich den Fokus auf die Sicherheit der Betriebsführung legt, umfasst die dem AEG unterstellte Eisenbahn-Bau- und Betriebsordnung (EBO) auch die Pünktlichkeit als Qualitätsziel der Betriebsführung. In EBO §47(2) wird vorgeschrieben, dass die Betriebsbeamten verpflichtet sind, für die sichere und pünktliche Durchführung des Eisenbahnbetriebs zu sorgen [68]. Im Gegensatz zu den gesetzlichen Vorgaben, die keine klare Aussage zu den Prioritäten der Betriebsqualität liefern, hat die Sicherheit bei einem Betreiber wie der Deutschen Bahn den absoluten Vorrang. Die Fahrdienstvorschriften der DB Netz AG in 408.0111 zu den Tätigkeiten im Bahnbetrieb fordert: „*Alle Mitarbeiter müssen in erster Linie für Sicherheit, dann für Pünktlichkeit des Bahnbetriebs*

sorgen.“ [69] Dadurch steht die Sicherheit stets im Mittelpunkt der Qualitätsziele der Betriebsführung.

2.3.5.3 Tätigkeitsfeld Ereignisbehandlung

Das dritte Tätigkeitsfeld in dem Rückfallebenenkonzept befasst sich mit der Ereignisbehandlung, welche genau dem Störungsmanagement in Abbildung 8 entspricht. Die Ereignisbehandlung hat die Aufgaben, tatsächliche Ereignisse und deren Ursache und Folge zu identifizieren, zu beheben sowie die voraussichtliche Einflussdauer des Ereignisses einzuschätzen. Die Aktivitäten „Kontrollieren“ und „Beheben“ im Störungsmanagement werden hier in diesem Abschnitt zur Vereinfachung der Darstellung als Teilaktivitäten der Aktivität „Behandeln“ zusammengefasst. Die voraussichtliche Einflussdauer des Ereignisses hat eine direkte Auswirkung auf die voraussichtliche Dauer der Betriebsführung in der Rückfallebene und ggf. die Absenkung des Leistungsniveaus zur Folge. Daher hat die Ereignisbehandlung das Qualitätsziel, die Einflussdauer des Ereignisses möglichst gering zu halten.

2.3.5.4 Wechselwirkung zwischen den Tätigkeitsfeldern

Um die erwünschte Betriebsqualität bezüglich des Leistungsniveaus, der Sicherheit und der Verfügbarkeit bei allen Ereignissen kundenorientiert und wirtschaftlich gerechtfertigt erzielen zu können, ist neben der eigentlichen Ausführungsqualität sowie der zulässigen und / oder kreativen Lösungsvielfalt des Rückfallebenenkonzepts auch ein optimaler Kommunikations- und Abstimmungsprozess zwischen den jeweiligen Aufgabenfeldern für den Erfolg eines Rückfallebenenkonzepts entscheidend. Jede Aktivität und deren Folge werden direkt oder indirekt Auswirkungen auf die Qualität und Möglichkeit der Ausführung einer anderen Aktivität haben können. In der Regel wird ein angesetztes Qualitätsziel eines Tätigkeitsfelds immer das erreichbare oder das mindeste Qualitätsniveau der anderen Tätigkeitsfelder direkt / indirekt beeinflussen. Dieser Einfluss lässt sich als eine Art sich verändernde Anforderung oder Rahmenbedingung darstellen, die auch während der Ausführung der Rückfallebenen dynamisch berücksichtigt werden soll.

Zum Beispiel soll die Betriebsleitung die eingeschätzte Einflussdauer der Ereignisbehandlung berücksichtigen, um ein optimales wirtschaftliches sowie kundenorientiertes Leistungsniveau nach Bedarf umplanen und disponieren zu können. Auf der anderen Seite soll die Betriebsleitung auch die Verfahrensgrenze der Betriebsführung bei der Umplanung und Disposition in Betracht ziehen, da die Anwendung einer bestimmten Rückfallebene bei der Betriebsführung eine gewisse Leistungsgrenze haben kann. Werden zu viele Züge an einen Ort geplant und disponiert, als es das bei der Betriebsführung angewandte Betriebsverfahren handlungstechnisch erlaubt, entsteht trotz der aktiven Betriebsleitung eine zusätzliche negative Auswirkung bei den Zügen. Nicht nur die erreichbare Behebungsdauer der Ereignisbehandlung kann die Planung und die Dispositionsentscheidung der Betriebsleitung beeinflussen, sondern auch umgekehrt bilden das Leistungsziel der Betriebsleitung und die dazu benötigten

Betriebsverfahren der Betriebsführung eine Entscheidungsgrundlage für die Festlegung der Prioritäten bei der Ereignisbehandlung.

2.3.6 Das Strukturprinzip des Rückfallebenenkonzepts

Basierend auf der bisherigen Herleitung kann das Rückfallebenenkonzept des Bahnbetriebs wie folgt zusammengefasst werden:

▪ Definition: *Rückfallebenenkonzept des Bahnbetriebs*

„Das Rückfallebenenkonzept des Bahnbetriebs ist ein System organisierter Qualitätskonzepte mit den entsprechenden Ausführungsvarianten und den Übergangsregeln, deren Qualitätsziele (Sicherheit, Leistungsniveau und Verfügbarkeit) von Fall zu Fall durch einen bestimmten Verhandlungsprozess zwischen den Tätigkeitsfeldern Betriebsleitung, Betriebsführung und Ereignisbehandlung gegenseitig abgestimmt werden sollen. Das Rückfallebenenkonzept dient vor allem dem Zweck, im Bahnbetrieb trotz des Einflusses aller vorgegebenen Unregelmäßigkeiten stets eine annehmbare kollektive Betriebsqualität erzielen zu können.“

Nach der obigen Definition lässt sich der Aufbau eines Rückfallebenenkonzepts in drei Arten von Strukturblocken spezifizieren. Dies sind die Ausführungsvariante, das Qualitätsziel und die Übergangsregeln, wie die Abbildung 10 darstellt. Die drei Arten von Strukturblocken enthalten zwar individuelle Elemente und unterschiedliche Zwecke, doch deren gegenseitiger Einfluss muss bei der Gestaltung eines Rückfallebenenkonzept stets zusammenhängend betrachtet werden.

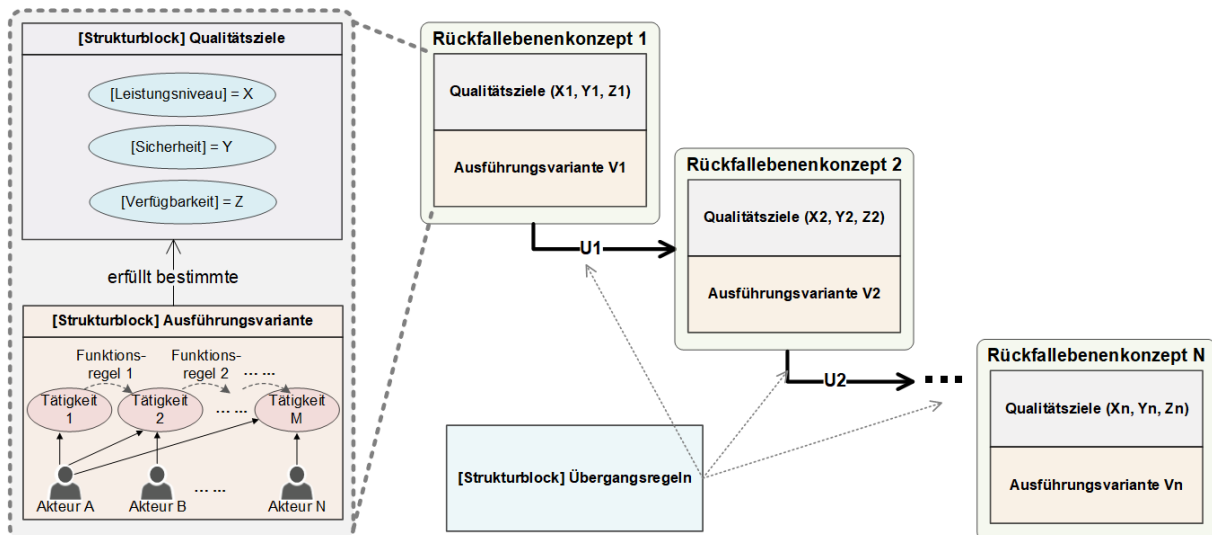


Abbildung 10: Schematische Darstellung des Strukturprinzips von Rückfallebenenkonzepten

2.3.6.1 Strukturblock Ausführungsvariante

Wie bereits in Kapitel 2.3.2 beschrieben wurde, kann eine Rückfallebene als eine Ausführungsvariante des Bahnbetriebs verstanden werden, die dazu dient, die vorgesehene Betriebsqualität trotz des Einflusses eines bestimmten Ereignisses möglichst weiter zu erbringen. Ungeachtet deren Einsatzbedingungen sowie deren erreichbarer Betriebsqualität lässt sich eine Ausführungsvariante strukturell / funktional in drei Elemente zerlegen. Dies sind die Tätigkeiten, Akteure und Funktionsregeln.

2.3.6.1.1 Element Tätigkeit

Das Element Tätigkeit hat den Zweck, den Umfang der Tätigkeiten einer Ausführungsvariante zu bestimmen. Wie in Abbildung 9 dargestellt ist, können alle Tätigkeiten in 6 Gruppen (Disponieren, Planen, Behandeln, Identifizieren, Sichern und Durchführen) zusammengefasst werden. Je nach dem Ereignis, den Einsatzbedingungen, dessen Folgen sowie dem vorgegebenen Qualitätsziel ergeben sich zur Realisierung des Bahnbetriebs in der Rückfallebene zwei Kombinationsmöglichkeiten von Tätigkeiten, und zwar mit oder ohne das Tätigkeitsfeld Betriebsleitung bzw. die Tätigkeiten Disponieren und Planen. Es wird vorausgesetzt, dass alle Varianten eines Rückfallebenenkonzepts immer das Ziel haben, den Bahnbetrieb wieder normalisieren zu wollen anstatt ihn stillzulegen. Demzufolge sind die zwei Tätigkeitsfelder Betriebsführung und Ereignisbehandlung sowie deren vier Tätigkeitsgruppen (Sichern, Durchführen, Behandeln und Identifizieren) die elementarsten und unverzichtbarsten Tätigkeiten der Rückfallebene. Im Gegensatz dazu sind die beiden Tätigkeitsgruppen (Disponieren und Planen) der Betriebsleitung als eine Art Optimierungsmaßnahme anzusehen, die dann von Fall zu Fall einzubeziehen sind.

2.3.6.1.2 Element Akteur

Der Akteur wird in der Ausführungsvariante benötigt, um die vorbestimmten Tätigkeiten ausführen zu können. Das Element Akteur hat deshalb den Zweck, die Verantwortung der einzelnen Tätigkeit(en) einer Ausführungsvariante mit den bestimmten Akteuren zu fixieren. Ein Akteur kann ein Mensch oder ein technisches System sein. Wichtig ist, dass der Akteur die Fähigkeit hat, die zugeteilte Tätigkeit eigenverantwortlich auszuführen. Bei der Aufteilung von Tätigkeiten auf die Akteure gibt es national und international unterschiedliche Prinzipien. Zum Beispiel liegt in Deutschland die Tätigkeitsgruppe „sichern“ bei der DB Netz AG, Anwendungsbereich Richtlinie 408, überwiegend in der Verantwortung des Fdl, während die Tätigkeitsgruppe „disponieren“ in der Verantwortung des Disponenten liegt. Im Gegensatz dazu sieht die Aufgabenteilung bei den nordamerikanischen Bahnen folgendermaßen aus: Auf Fernsteuerstrecken liegen sowohl die Tätigkeit „sichern“ als auch die Tätigkeit „disponieren“ überwiegend in der Verantwortung derselben Person, die als Dispatcher bekannt ist [70]. Ein weiteres Beispiel des international unterschiedlichen Aufteilungsprinzips ist das „Permissive Fahren“, in dem der Tf ohne besonderen Auftrag des Fdl oder Dispatcher an Hauptsignalen, die nur der Zugfolgeregelung dienen, bei Haltestellung vorsichtig auf Sicht weiterfahren darf. In

diesem Fall geht die Verantwortung „sichern“ in der Rückfallebene dann vom Fdl / Dispatcher auf den Tf über. Das permissive Fahren ist international das dominierende Standardverfahren in der Rückfallebene auf Strecken mit selbststätigem Streckenblock, was aber in Deutschland derzeit im Geltungsbereich der EBO nicht erlaubt ist [70–72]. Darüber hinaus kann ein Akteur in einer Ausführungsvariante gleich mehrere Tätigkeiten haben, wie z. B. der Dispatcher der nordamerikanischen Bahnen oder auch der Fdl in Deutschland, der im Fall einer Störung von Blockeinrichtungen neben der Tätigkeit „sichern“ auch die Grundstellung von Blockeinrichtungen unter der Tätigkeit „behandeln“ eigenständig herstellen darf [69]. Im umgekehrten Fall ist es auch möglich, eine Tätigkeit auf mehrere Akteure zu verteilen. Zum Beispiel kann der Fdl in Deutschland im Fall einer Räumungsprüfung die Feststellung der Zugvollständigkeit im Rahmen seiner Tätigkeit „sichern“ durch den Tf, einen Zugschlussmeldeposten oder einen benachbarten Fdl bestätigen lassen [69, 72]. Die Beispiele zeigen, dass sich durch die Kombination von Tätigkeiten und Akteuren, auch für ein gleiches Ereignis, eine Vielzahl von unterschiedlichen Ausführungsvarianten ergeben kann. Aufgrund der unterschiedlichen technischen, organisatorischen und qualitativen Auslegung der Bahnen sowie ihrer unterschiedlichen Sicherheitsphilosophie gibt es derzeit im Allgemeinen kein einheitliches Aufteilungsprinzip.

2.3.6.1.3 Element Funktionsregel

Neben den Elementen Tätigkeit und Akteur hat das letzte Element Funktionsregel die Aufgabe, die Kombination Tätigkeit-Akteur in einen Prozess umzuwandeln, damit die Ausführungsvariante qualitätsgemäß erbracht werden kann. Mit der Funktionsregel soll vor allem folgende Frage beantwortet werden: „Wie gestalte ich den Prozess richtig, damit die Ausführungsvarianten qualitätsgemäß funktionieren?“ Im Vergleich dazu befindet sich die Übergangsregel (siehe Kapitel 2.3.6.3) auf einer strukturell höheren Ebene im Rückfallebenenkonzept im Hinblick auf die gesamte Qualität des Bahnbetriebs. D. h., die Funktionsregel schreibt vor, in welcher Reihenfolge die Kombinationen Tätigkeit-Akteur einer Ausführungsvariante unter dem angesetzten Qualitätsziel ausgeführt werden muss. Zum Beispiel darf der Fdl in Deutschland zwar die Grundstellung einer Blockeinrichtung eigenständig herstellen, jedoch muss der Fdl nach der Funktionsregel vor der Grundstellung eine Räumungsprüfung für den zuletzt gefahrenen Zug durchführen [69]. Diese Funktionsregeln werden heute bei den meisten Bahnen im Allgemeinen als „Betriebliche Regeln“, oder auf Englisch: „Operational Rules“, bezeichnet. Auch zur Dokumentation von Funktionsregeln gibt es international unterschiedliche Ansätze, zumindest bei den Tätigkeiten Sichern und Durchführen bzw. bei den sicherheitsrelevanten Funktionsregeln. Während im deutschsprachigen Raum die funktionsorientierte Darstellungsart dominiert, werden die Funktionsregeln in Großbritannien prozessorientiert dargestellt [73]. In Deutschland sind diese allgemeinen Funktionsregeln in der Sammlung des betrieblich-technischen Regelwerks der DB Netz AG enthalten, z. B. in der Modulgruppe 408.01-06 für den Fahrdienstleiter und Weichenwärter und der Modulgruppe 408.21-26 für den Triebfahrzeugführer zum Thema Züge

fahren sowie in der Richtlinie 420 für den Dispatcher zum Thema Disposition in Betriebszentralen.

2.3.6.2 Strukturblock Qualitätsziel

Eine Ausführungsvariante hat unter der vorgegebenen Einsatzbedingung eine bestimmte Qualitätsgrenze. Auch kann ein bestimmtes Qualitätsziel durch mehrere Ausführungsvarianten erreicht werden. Der zweite Strukturblock Qualitätsziel hat den Zweck, die möglichen Ausführungsvarianten im Rückfallebenenkonzept anhand der erreichbaren Betriebsqualitäten und vorgesehenen Einsatzbedingungen zu systematisieren. Mit dieser Zuordnung soll den Anwendern des Rückfallebenenkonzepts ermöglicht werden, die Qualitätsgrenze einer Ausführungsvariante unter bestimmten Einsatzbedingungen zu erkennen oder umgekehrt die möglichen Ausführungsvarianten, durch deren Anwendung ein bestimmtes Qualitätsziel erreicht werden kann, zu überblicken. Wie das Beispiel Räumungsprüfung in Kapitel 2.3.6.1 zeigt, kann sich der Fdl die Feststellung der Zugvollständigkeit gleich durch drei unterschiedlichen Akteure bzw. Ausführungsvarianten bestätigen lassen. Es mag sein, dass sich die drei Ausführungsvarianten bezüglich ihrer Sicherheit kaum unterscheiden. Wird aber das erreichbare Leistungsniveau in Betracht gezogen, kann bei der Bestätigung durch den benachbarten Fdl im Fall einer zentralisierten Fahrdienstleitung und der daraus folgenden großen Entfernung zwischen beiden Fdl im Vergleich zur Bestätigung durch den Tf nur eine niedrige Betriebsdichte erreicht werden. Wie in [74] berichtet wird, sind solche Kennzeichnungen der Betriebsqualität im heutigen Rückfallebenenkonzept im betrieblich-technischen Regelwerk der DB Netz AG weitgehend nicht zu erkennen. Die Tatsache lässt sich bisher rational argumentieren. Da jede zulässige Ausführungsvariante nach den gesetzlichen Regelungen ein Mindestniveau der Sicherheit nicht unterschreiten darf und ausschließlich unter der Betrachtung von Safety-Ereignissen entwickelt wurde, deren Umfeld seit Jahrzehnten recht stabil und homogen ist, ist es bisher nicht notwendig, die Sicherheit jeder Variante mit deren Einsatzbedingungen spezifisch zu berücksichtigen. Auch die Kennzeichnung von Leistungsniveau und Verfügbarkeit ergibt sich bisher als überflüssig, da das Ausmaß und die Häufigkeit einer Störung im heutigen modernen, hochzuverlässigen Bahnsystem unter der ausschließlichen Betrachtung von Safety- Ereignissen durchaus geringfügig ist.

2.3.6.3 Strukturblock Übergangsregel

Im Gegensatz zu den Funktionsregeln einer Ausführungsvariante (siehe Kapitel 2.3.6.1) beschäftigt sich die Übergangsregel mit der Frage: „Wie kombiniere ich die unterschiedlichen Qualitätsziele und die möglichen Ausführungsvarianten richtig, damit eine annehmbare kollektive Betriebsqualität erreicht werden kann?“ Die Übergangsregel hat daher grundsätzlich die Aufgabe, das identifizierte Ereignis dem vorgesehenen Qualitätsziel und der geeigneten Ausführungsvariante zuzuweisen und deren Übergänge zu regeln. Die erste Aufgabe der Zuweisung setzt eine zuverlässige Offenbarung eines Ereignisses voraus, was nach der Eingrenzung der Aufgabenbereiche von Rückfallebenen in Kapitel 2.3.4 außerhalb des Kontextes eines Rückfallebenenkonzepts liegt. An dieser Stelle verbindet die Übergangsregel

lediglich das offenbarte Ereignis mit der Ausführungsvariante. Zum Beispiel werden den Ereignissen im Störungsmanagement in Richtlinie 420 der DB Netz AG in den Betriebsleitzentralen je nach Ausmaß des Ereignisses (A: Störungen mit erheblichen Auswirkungen; B: Störungen mit außergewöhnlichen Auswirkungen; C: Eskalierte Situation) unterschiedliche Ausführungsvarianten zugewiesen [67].

Die Übergangsregel verbindet nicht nur das erste Ereignis mit der Ausführungsvariante, welches als die erste Ursache zur Einführung einer Rückfallebene identifiziert wurde. Ebenfalls regelt die Übergangsregel den Übergang zwischen dem Zwischenereignis und der weiteren Ausführungsvariante. Das Beispiel zur Grundstellung von Blockeinrichtungen aus Kapitel 2.3.6.1. kann hier fortgesetzt werden. Nach der Funktionsregel darf der Fdl zwar nach einer Einzelräumungsprüfung die Grundstellung einer Blockeinrichtung herstellen, jedoch muss er nach zwei erfolglosen kompletten Durchläufen (Räumungsprüfung, Grundstellung, Züge fahren lassen) die Räumungsprüfung auf Zeit einführen. Die Übergangsregel schreibt an dieser Stelle vor, dass der Fdl nach zwei erfolglose Versuche zur einen anderen Ausführungsvariante übergehen muss. In diesem Fall hat die Ausführungsvariante für den Fdl bezüglich der Tätigkeit Sichern (Einzelräumungsprüfung) zwar nicht geändert, lediglich die Anwendungsdauer der Tätigkeit hat nach dem neuen Qualitätsziel verlängert (Räumungsprüfung auf Zeit). Es entfällt jedoch bei dem Fdl in der neuen Variante die Tätigkeit Behandeln (Grundstellung von Blockeinrichtung). Die Tätigkeit der Behandlung wechselt dann nach der Übergangsregel z. B. zu dem technischen Mitarbeiter, was aber nicht in referenzierten Richtlinie für den Fdl näher beschrieben wurde. Letztendlich ist der Strukturblock Übergangsregel für eine hochqualitative Zusammensetzung von Rückfallebenenkonzepten entscheidend. Da ein Rückfallebenenkonzept ohne die korrekte Zuweisung von Ereignis zu der Ausführungsvariante sowie die optimale Zusammenstellung von Ausführungsvariante, Qualitätsziel und deren Übergangskriterien nicht oder ggf. nur hemmend funktionieren kann.

3 Die Bewertungssystematik und deren Anwendungsprinzipien

3.1 Anforderungen an die Bewertungssystematik

3.1.1 Die Herausforderung des künftigen Störungsbetriebs

Wenn die Technik nicht mehr oder nur teilweise funktioniert, haben die menschlichen Akteure in den Rückfallebenen des Bahnbetriebs die Aufgabe, den Bahnbetrieb unter eigener Verantwortung mit oder ohne technische Unterstützung fortzuführen. Um bei Störungen den Bahnbetrieb fortführen zu können, muss das Rückfallebenenkonzept so bereitgehalten werden, dass z. B. für den Fahrdienstleiter und den Triebfahrzeugführer klare Anweisungen für die Handlungen vorliegen. Im Vergleich zu Großbritannien, wo die Regeln der Rückfallebene als prozessorientiertes Darstellungsprinzip verfolgt werden, wird in Deutschland das funktionsorientierte Darstellungsprinzip angewandt. D. h., in den Regeln der Rückfallebene in Deutschland wird nirgends geschlossen beschrieben, wie die Tätigkeiten in der Rückfallebene bezüglich einer Zugfahrt von A nach B Schritt für Schritt prozessorientiert durchzuführen sind. Es wird vorausgesetzt, dass die Menschen ein fundiertes Verständnis über die Zusammenhänge zwischen den Prozessschritten besitzen und die Tätigkeiten in der Rückfallebene fertigkeitstbasiert ausführen können [73, 74].

Wie in [75] beschrieben, geraten die Menschen durch die zunehmende Automatisierung und Digitalisierung nach und nach in den Hintergrund des Betriebsablaufs. Die Menschen haben heutzutage im normalen automatisierten Betrieb häufig nur eine passive Überwachungsfunktion. Die Forschung von Bainbridge [76] hat gezeigt, dass Menschen für das zuverlässige, dauerhafte Ausführen von Überwachungsaufgaben schlecht geeignet sind. Bei der passiven Überwachung der Betriebsabwicklung nimmt der Mensch im Vergleich zur aktiven Teilnahme weniger Informationen auf. Die Situation wird kritisch, wenn die Menschen auf einmal von der passiven Überwachung auf eine aktive Teilnahme am sicherheitsrelevanten Betriebsablauf wechseln müssen. Diese steigende Passivität verursacht beim Menschen nicht nur ein potenzielles Informationsdefizit über den aktuellen Betriebszustand in der aktiven Teilnahme. Auch dessen Handlungssicherheit geht im Trend der technischen Entwicklung von der bisherigen Annahme einer fertigkeitstbasierten Handlung zurück auf eine regelbasierte Handlung [77, 78]. Infolgedessen wird die Handlungssicherheit von Menschen in der Rückfallebene mit den Fortschritten der Systementwicklung kontraproduktiv reduziert, wie auf der linken Hälfte der Wirkungskette in Abbildung 11 dargestellt wird.

Unfälle und Vorfälle in der Vergangenheit haben gezeigt, dass der Betrieb in der Rückfallebene für den Fehler des Menschen anfällig ist. Was aber bisher in dem durch Safety-Ereignisse geprägten Rückfallebenenkonzept nicht berücksichtigt wurde, sind die Fälle mit den Charakteren eines IT-Angriffs. Aufgrund der rasanten Entwicklung der IT wird das System Bahn bereits ständig von neuen Angriffstechniken bedroht. Zusätzlich hat das System Bahn mit seiner zunehmenden IT-Vernetzung und der IT-basierten Steuerung ständig neue potenzielle

Zugangspunkte für den Angreifer erschaffen. Dies könnte zur Folge haben, dass das System Bahn häufig angegriffen würde und dessen Betrieb häufig in den Rückfallebenen durchgeführt werden müsste. Neben der Häufigkeit kann das Ausmaß eines IT-Angriffs aufgrund der IT-Vernetzung deutlich größer sein als ein typisches Safety-Ereignis. Es kann z. B. eine längere Reparaturdauer bzw. Betriebsdauer in der Rückfallebene zur Folge haben, größere räumliche Bereiche gestört werden sowie eine höhere Anzahl von Systemen und Funktionen betroffen sein.

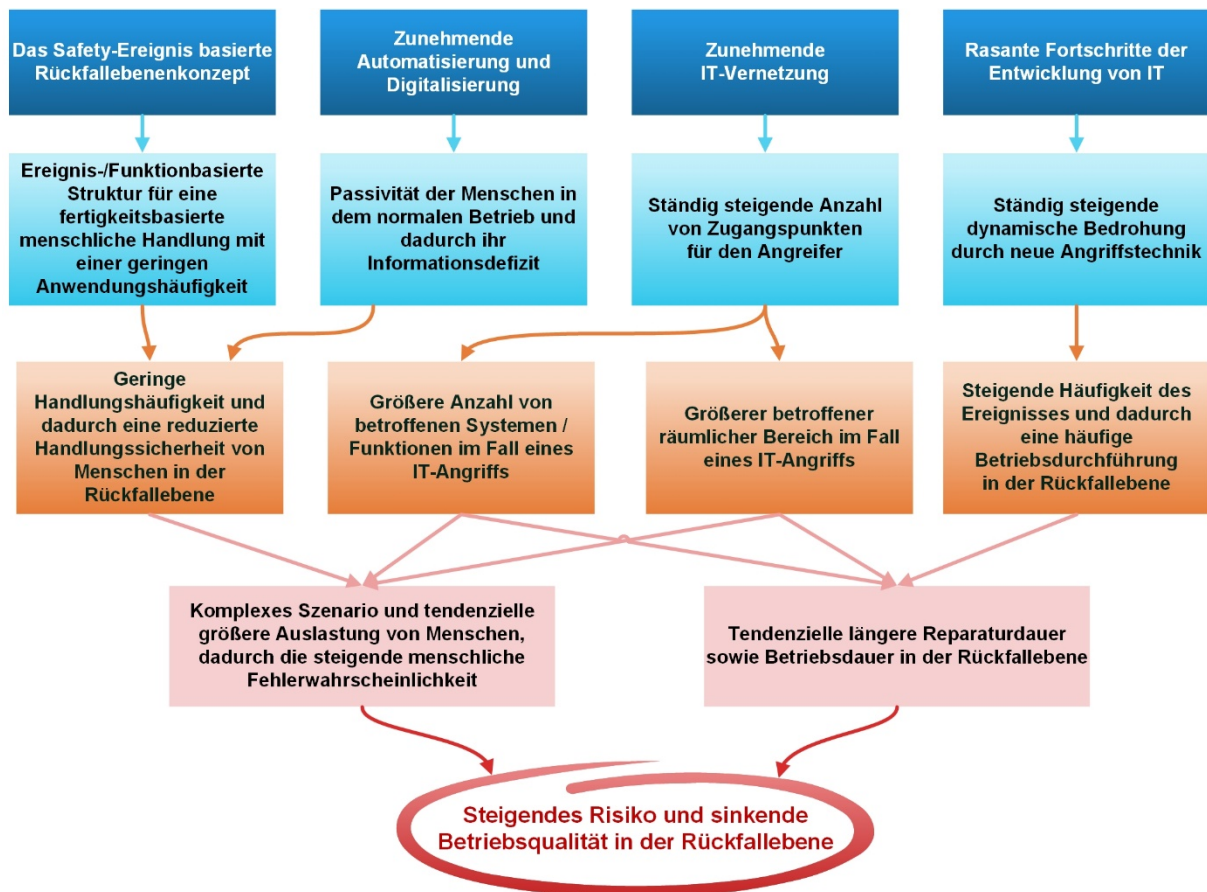


Abbildung 11: Wirkungskette eines IT-Angriffs auf die Rückfallebene im Bahnbetrieb

Häufig wird zum Zweck einer kürzeren Behebungsdauer bei den häufig auftretenden Ereignissen die Tätigkeit Behandlung dem gleichen Akteur überlassen, der auch für die Betriebsführung verantwortlich ist. Z. B. kann der Fdl in Deutschland heute in der Rückfallebene die Störung eigenverantwortlich durch eine Hilfshandlung im ESTW beheben. Dies bedeutet auch, dass sich die Behandlung eines Ereignisses stärker auf denselben menschlichen Akteur mit der Verantwortung der Betriebsführung konzentriert, je häufiger ein Ereignis auftritt. Werden in der Zukunft bestimmte Ereignisse durch den IT-Security-Angriff häufig auftreten, dann ist zu erwarten, dass deren Behandlungen, z. B. zusätzliche Authentifizierungsvorgänge oder einfache IT-Security-Auditierungen, zu Gunsten einer kürzeren Behandlungsdauer direkt vom menschlichen Akteur der Betriebsführung ausgeführt werden, anstatt vorher einer sorgfältigen Untersuchung der technischen Mitarbeiter der

Ereignisbehandlung unterzogen werden zu müssen. Dies hat zur Folge, dass der menschliche Akteur der Betriebsführung in der Rückfallebene zukünftig deutlich mehr Aufgaben mit komplexeren Regeln beherrschen müsste als heute, da zusätzlich auch neue Prozessschritte und Bedingungen zur Behandlung von Security-Ereignissen zu erwarten sind.

Wissenschaftliche Untersuchungen haben bereits gezeigt, dass nicht nur die Häufigkeit der Aufgabe, sondern auch z. B. der Umfang, die Variabilität und die Dauer der Aufgabe sowie die Größe des Aufgabenbereichs die Fehlerwahrscheinlichkeit der Menschen bei der Handlung signifikant beeinflussen können [77, 79, 80]. Im Endeffekt wird künftig für die menschlichen Akteure eine deutlich höhere Komplexität und Arbeitsbelastung in der Rückfallebene des Bahnbetriebs durch die Bedrohung der IT-Security-Angriffe erwartet. Auch wenn die Passivität der Menschen und die daraus folgende Handlungsunsicherheit durch die steigende Nutzung der Rückfallebene sich gewissermaßen ausgleichen könnten, lässt sich der Einfluss der Komplexität und des Ausmaßes der Störungslage nach einem IT-Security-Angriff nur bedingt wettmachen. D. h., falls das Rückfallebenenkonzept des Bahnbetriebs unverändert bleibt, dann ist zu erwarten, dass im künftigen Bahnbetrieb in der Rückfallebene nach dem jetzigen, in Abbildung 11 dargestellten Trend der IT-Entwicklung mit einem steigenden Risiko und einer sinkenden Betriebsqualität gerechnet werden muss.

Es ist daher bei der Gestaltung eines Rückfallebenenkonzepts eine Herausforderung, die Charakteristiken eines IT-Security-Angriffs, die erwünschte Betriebsqualität sowie die Tätigkeitsgrenze der Menschen zusammenhängend zu berücksichtigen. Um die Qualitäten des Bahnbetriebs systematisch analysieren, bewerten und miteinander vergleichen zu können, steht die Entwicklung einer Systematik zur Bewertung von Betriebsqualitäten des Rückfallebenenkonzepts im Mittelpunkt dieser Arbeit. Bei der Gestaltung der Bewertungssystematik wird das Grundprinzip verfolgt, dass auch die Charakteristiken eines IT-Angriffs und deren Folge auf die menschliche Auslastung in der Bewertung zusammenhängend berücksichtigt werden.

3.1.2 Berücksichtigung der Charakteristiken des IT-Angriffs

Aus der Wirkungskette eines IT-Angriffs auf den Bahnbetrieb in Abbildung 11 lässt sich entnehmen, dass die Auswirkungen eines IT-Angriffs mindestens die folgenden Charakteristiken besitzen:

- Zum Ausmaß:
 - Voraussichtlich können mehr Betriebsfunktionen betroffen sein
 - Voraussichtlich können größere geografische Bereiche betroffen sein
- Zur Dauer:
 - Voraussichtlich kann eine längere Störungsdauer erwartet werden
- Zur dynamische Bedrohungslage:
 - Voraussichtlich kann ein häufigeres Auftreten von Störungen erwartet werden

Da die Bewertungssystematik die Charakteristiken eines IT-Angriffs berücksichtigen soll, lassen sich die Anforderungen an die Bewertungssystematik sowie die benötigten Variablen aus den obigen Charakteristiken ableiten. Um das Ausmaß der betroffenen Betriebsfunktionen in der Bewertung berücksichtigen zu können, sollte die Bewertungssystematik in der Lage sein, die Art sowie die Anzahl der betroffenen Betriebsfunktionen generisch abzubilden. Dazu müssen die relevanten Betriebsfunktionen, die für die Bewertung der Betriebsqualität relevant sind, im Vorfeld als Variablen identifiziert und aufgenommen werden. Neben dem Ausmaß der betroffenen Funktionen haben auch die Größe des betroffenen Bereichs sowie die Störungsdauer einen großen Einfluss auf die Betriebsqualität des Rückfallebenenkonzepts. Die Bewertungssystematik sollte daher auch die Anforderungen erfüllen, dass die Größe des betroffenen Bereichs und die Betriebsdauer der Störung als Variablen in der Bewertung enthalten sind.

Bei der letzten Anforderung bezüglich der Bewertung der Charakteristik eines IT-Angriffs handelt es sich um die Berücksichtigung der dynamischen Bedrohungslage eines IT-Umfelds. Die Bedrohungslage, in der sich ein System zum Zeitpunkt der Analyse befindet, ist aber abhängig von dem aktuellen IT-Schutzniveau des Systems sowie der Stärke des IT-Angriffs. Dies bedeutet, dass ein Angriff für ein System in einem stärkeren Schutzzustand als unbedeutend angesehen werden könnte, während derselbe IT-Angriff für ein System in einem schwächeren Schutzzustand als höhere Bedrohung eingestuft wird. Die Bewertungssystematik sollte daher bei der Ermittlung der Bedrohungslage sowohl die Stärke des IT-Schutzniveaus als auch die Stärke des IT-Angriffs als Variable enthalten. Eine Übersicht der Charakteristik eines IT-Angriffs und die daraus resultierenden Anforderungen sowie die benötigten Variablen für die Bewertungssystematik befindet sich in Tabelle 2.

Tabelle 2: Charakteristik des IT-Angriffs und die Anforderungen an die Systematik

Einflussfaktoren	Anforderungen	Benötigte Variable
Charakteristik des IT-Angriffs	Die Bewertungssystematik sollte...berücksichtigen	Die Bewertungssystematik sollte die Variable...enthalten
Ausmaß (Mehr Funktionen betroffen)	→ die Art und Anzahl der betroffenen Betriebsfunktionen	[Generische Betriebsfunktion]
Ausmaß (Größere Bereiche betroffen)	→ die Größe des betroffenen Bereichs	[Größe des betroffenen Bereichs]
Dauer (Längere Betriebsdauer)	→ die Dauer der Störung	[Betriebsdauer]
Dynamische Bedrohungslage	→ die Lage der dynamischen Bedrohung	[Stärke des IT-Schutzniveaus], [Stärke des IT-Angriffs]

3.1.3 Berücksichtigung der menschlichen Auslastung

Neben dem Einfluss des IT-Angriffs hat die Wirkungsanalyse in Abbildung 11 ebenfalls gezeigt, dass das Zusammenwirken der Passivität der Menschen und der Charakteristiken des IT-Angriffs zu einer Reduzierung der Betriebssicherheit im Störungsbetrieb führen kann. Die Bewertungssystematik sollte daher die Anforderung erfüllen, dass im Zuge der Bewertung auch

die menschliche Auslastung berücksichtigt wird. Aus den Charakteristiken des IT-Angriffs lassen sich die folgenden drei Faktoren, die sich negativ auf die menschliche Auslastung im Störungsbetrieb auswirken können, ableiten. Bei diesen drei Faktoren handelt es sich um die Dauer der Handlung, den Umfang der Handlung und die Intensität der Handlung.

Der Umfang der Handlung beschäftigt sich mit der Frage: „Wie viele Handlungen muss der Mensch während der Störung von der Technik übernehmen?“. Daraus lässt sich der Umfang der Handlung z. B. direkt aus den betroffenen Betriebsfunktionen, welche während der Störung durch die Teilnahme der Menschen ausgeführt werden müssen, auszählen. Um den Umfang der Handlung der Menschen in der Störung einschätzen zu können, muss neben den betroffenen Betriebsfunktionen auch der maßgebliche Akteur einer Betriebsfunktion bzw. einer Handlung in der Bewertungssystematik differenzierbar sein. Der Akteur der Betriebsfunktion wird daher als Variable in der Bewertung benötigt, um die Verantwortlichkeit jeder Betriebsfunktion bei der Bewertung voneinander unterscheiden zu können. Diese Differenzierung wird außerdem auch benötigt, um die Sicherheit des Betriebs korrekt ermitteln zu können, da jeder Akteur bzw. jede Funktion unterschiedliches Versagenspotenzial haben kann.

Der zweite Faktor, die Intensität der Handlung, befasst sich mit der Frage: „Wie viele Handlungen muss der Mensch innerhalb eines betrachteten Zeitraums ausführen?“. Im Gegensatz zum Umfang der Handlung, der lediglich auf die Anzahl der Art von Funktionen fokussiert, steht bei der Intensität der Handlung die Anzahl der Handlungen, die innerhalb eines bestimmten Zeitraums vom Menschen ausgeführt werden müssen, im Fokus der Betrachtung. Die Intensität der Handlung kann auch als die Frequenz der Handlung verstanden werden. Wenn bei einer gleichartigen Störung der betroffene Bereich größer wird, die Anzahl der zuständigen menschlichen Akteure im Bereich jedoch identisch bleibt, dann ändert sich der Umfang der Handlung zwar nicht, doch die Intensität der Handlung steigt proportional mit der Größe des betroffenen Bereichs. Das heißt aber auch, dass die Intensität der Handlung nicht nur von der Größe des betroffenen Bereichs, sondern auch von der Anzahl der menschlichen Akteure abhängig ist. Zusätzlich muss beachtet werden, dass auch die Betriebsdichte einen Einfluss auf die Intensität der Handlung haben kann. Je mehr Zugfahrten innerhalb eines bestimmten Zeitraums während der Störung stattfinden, desto häufiger muss der menschliche Akteur die gleiche Handlung ausführen. Schließlich benötigt die Bewertungssystematik die Variablen Betriebsdichte, Größe des betroffenen Bereichs und die Anzahl der Akteure, um die Intensität der Handlung in der Bewertung abbilden zu können.

Der letzte Faktor, der die menschliche Auslastung beeinflussen kann, ist die Dauer der Handlung. Dieser Faktor beschäftigt sich mit der Frage: „Wie viele Stunden muss der Mensch im Störungsbetrieb arbeiten?“. Um die Dauer der Handlung in der Bewertung berücksichtigen zu können, wird die Einsatzstunde der menschlichen Akteure im Störungsbetrieb als Variable in die Bewertungssystematik aufgenommen. Die Variable Einsatzstunde betrifft im Rahmen dieser Arbeit lediglich die menschlichen Akteure, die während des Regelbetriebs nicht aktiv an den sicherheitsrelevanten betrieblichen Handlungen teilnehmen, sondern erst im Störungsbetrieb aktiv agieren müssen. Dies sind z. B. die Fahrdienstleiter. Eine Übersicht der

Einflussfaktoren auf die menschliche Auslastung und die daraus resultierenden Anforderungen sowie die benötigten Variablen für die Bewertungssystematik befindet sich in Tabelle 3.

Tabelle 3: Einflussfaktoren auf die menschliche Auslastung und die Anforderungen an die Systematik

Einflussfaktoren	Anforderungen	Benötigte Variable
Menschliche Auslastung	Die Bewertungssystematik sollte...berücksichtigen	Die Bewertungssystematik sollte die Variable...enthalten
Umfang der Handlung	→ den Umfang der menschlichen Handlung	[Generische Betriebsfunktion], [Akteur der Betriebsfunktion]
Intensität der Handlung	→ die Frequenz der menschlichen Handlung	[Betriebsdichte], [Größe des betroffenen Bereichs] [Anzahl der Akteure]
Dauer der Handlung	→ die Einsatzdauer der Menschen	[Einsatzdauer im Störungsbetrieb]

3.1.4 Berücksichtigung der Qualitätsmerkmale des Bahnbetriebs

Um das Ergebnis der Bewertung zwischen den unterschiedlichen Rückfallebenenkonzepten vergleichen zu können, wird auch bei der Bewertungssystematik eine vergleichbare Basis zur Aussage der Betriebsqualität benötigt. Wie in Kapitel 2.3.2 beschrieben, liegt die Stärke der Bahn im Vergleich zu den anderen Verkehrsmitteln im Bereich Landverkehr in drei ausschlaggebenden Qualitätsmerkmalen. Dies sind nämlich ihre hohe Sicherheit, ihr hohes Leistungsniveau und ihre hohe Verfügbarkeit. Da ein Rückfallebenenkonzept den Zweck hat, im Bahnbetrieb trotz des Einflusses aller vorgegebenen Unregelmäßigkeiten stets eine annehmbare kollektive Betriebsqualität erzielen zu können, sollte die Bewertungssystematik auch in der Lage sein, die drei Qualitätsmerkmale des Bahnbetriebs zum Zweck des Vergleichs entsprechend zu ermitteln.

Die Sicherheit des Bahnbetriebs wird wie in Kapitel 2.1 beschrieben, weitgehend durch das Konzept Risiko dargestellt, in dem das Risiko als „*Kombination aus erwarteter Häufigkeit eines Schadens und erwartetem Schweregrad dieses Schadens*“ definiert wird. Wie in Abbildung 4 dargestellt ist, ist der Schaden die Folge eines betrieblichen Ereignisses, dessen Auftreten eine Betriebsgefahr auslösen kann. Im Laufe dieser Arbeit werden solche betrieblichen Ereignisse, die zu einer Betriebsgefahr führen können, unabhängig von ihrer Ursache einheitlich als Versagen bezeichnet. Das System Bahn ist ein Mensch-Technik-System, insbesondere bei dessen Betrieb während der Störung, wo Teile der Funktionen der modernen technischen Systeme durch die Menschen ersetzt werden müssen. Es ist daher notwendig, die Wahrscheinlichkeit des Eintretens eines Versagens in der Bewertung nach Menschen und Technik zu differenzieren. Um das Risiko des Bahnbetriebs ermitteln zu können, muss die Bewertungssystematik daher sowohl die Versagensrate der Technik als auch die Versagenswahrscheinlichkeit der Menschen als Variablen haben. Zusammen mit der Variable Schadensausmaß des Versagens kann das Risiko eines Rückfallebenenkonzepts durch die Bewertungssystematik ermittelt werden.

Neben der Sicherheit des Bahnbetriebs steht das Leistungsniveau des Bahnbetriebs ebenfalls im Mittelpunkt des Qualitätsvergleichs von Rückfallebenenkonzepten. Wie in Kapitel 2.3.1 beschrieben, hat die Bahn als Kritische Infrastruktur in Deutschland die Verantwortung, ihre Funktionalität während der Störung angemessen aufrechtzuerhalten. Dazu gehört neben der Sicherheit auch ein angemessenes Leistungsniveau. Unter dem Begriff Leistungsniveau des Bahnbetriebs verbergen sich zwei Aspekte. Dies sind die Betriebsdichte und die Beförderungsgeschwindigkeit. Bei der Betriebsdichte handelt es sich um den Durchsatz der Züge je Zeiteinheit im Bereich der Betrachtung. Bei einem maximal möglichen Durchsatz einer Betriebsanlage unter einer bestimmten Struktur des Betriebsprogramms wird diese Betriebsdichte als maximale Leistungsfähigkeit bezeichnet. Wie nach der Theorie der Wartezeitfunktion in [72] beschrieben, nimmt die mittlere Beförderungsgeschwindigkeit der Züge auf einer Betriebsanlage mit steigender Betriebsdichte ab und erreicht bei der maximalen Leistungsfähigkeit den Wert Null. Das bedeutet zwar nicht, dass alle Züge bei maximaler Betriebsdichte stillstehen. Da nach der Theorie jedoch die mittlere Wartezeit bei maximaler Betriebsdichte gegen Unendlich geht, konvergiert die mittlere Beförderungsgeschwindigkeit gegen Null, wie in Abbildung 12 schematisch dargestellt wird. Daher muss bei der Gestaltung des Leistungsniveaus des Bahnbetriebs sowohl die Beförderungsgeschwindigkeit als auch die Betriebsdichte zusammenhängend berücksichtigt werden. Infolgedessen wird das Leistungsniveau des Rückfallebenenkonzepts im Rahmen der Bewertungssystematik anhand der Beförderungsenergie dargestellt, die nach [72] als „*Produkt aus der in Zügen je Zeiteinheit gemessenen Belastung und der mittleren Beförderungsgeschwindigkeit einer Teilstrecke*“ definiert wird. Dadurch wird die Qualität des Leistungsniveaus zugleich von der Betriebsdichte und der Beförderungsgeschwindigkeit abhängig gemacht und kann zusammenhängend betrachtet werden.

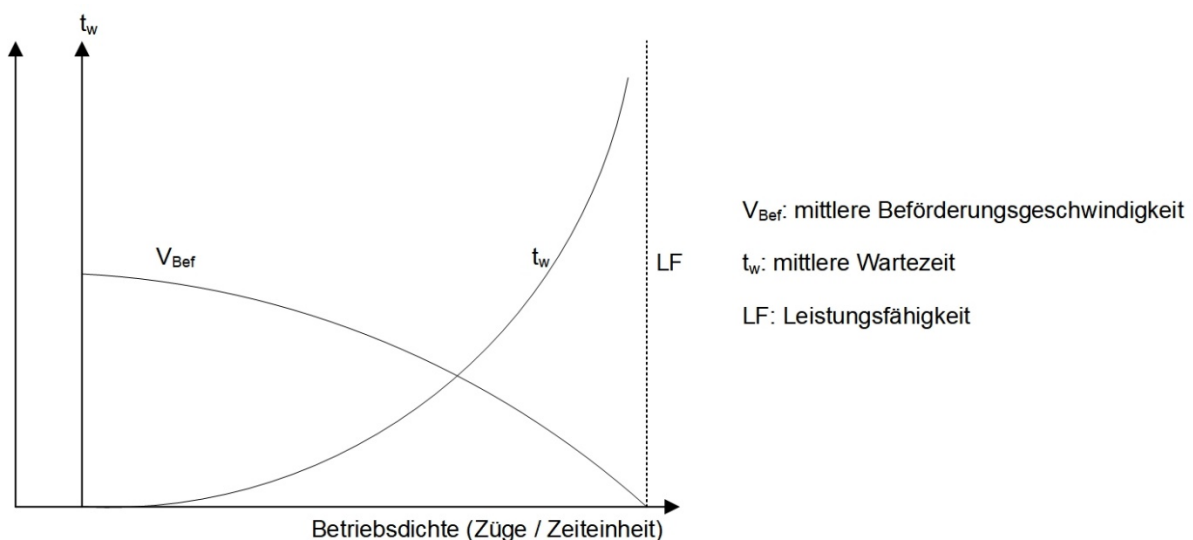


Abbildung 12: Wechselwirkung der Beförderungsgeschwindigkeit und Betriebsdichte nach [72]

Das dritte Qualitätsmerkmale des Bahnbetriebs, welches die Abbildung 7 zeigt, ist die Verfügbarkeit des Systems. Im Rahmen dieser Arbeit wird zwischen der betrieblichen

Verfügbarkeit und der technischen Verfügbarkeit unterschieden. Bei der Betrachtung der betrieblichen Verfügbarkeit wird das System als verfügbar angesehen, solange der Bahnbetrieb im Bereich der Betrachtung nicht komplett stillsteht. Das bedeutet, wenn der Bahnbetrieb im Fall einer Störung unter der Anwendung eines Rückfallebenenkonzepts weiter durchgeführt werden kann, obwohl das Risiko vielleicht höher und das Leistungsniveau niedriger als im Regelbetrieb ist, gilt das System Bahn im Kontext der betrieblichen Verfügbarkeit weiterhin als verfügbar. Im Vergleich dazu werden alle Zeiten im Kontext der technischen Verfügbarkeit als nicht verfügbar angesehen, solange eine Unregelmäßigkeit im System vorhanden ist und der Bahnbetrieb sich nicht komplett im automatisierten Regelbetrieb befindet. Das heutige Eisenbahnsystem hat eine Vielzahl von Konzepten und Ersatzhandlungen, mit denen beim Eintreten einer Störung der Betrieb weiter fortgesetzt werden kann. Mit der Anwendung der betrieblichen Verfügbarkeit können die Unterschiede der Verfügbarkeit bei dem modernen System nicht kenntlich gemacht werden. Solange der Bahnbetrieb nicht komplett stillsteht, hat das System im Zeitraum der Betrachtung stets eine Verfügbarkeit von 100%. Aus diesem Grund wird im Rahmen der vorliegenden Bewertungssystematik bei der Betrachtung der Verfügbarkeit die technische Verfügbarkeit herangezogen. Durch die technische Verfügbarkeit kann die Qualität des Systems deutlich differenziert werden. Solange sich der Betrieb nicht im automatisierten Zustand befindet und die aktive Teilnahme von Menschen an der sicherheitsrelevanten Handlung erforderlich ist, werden die Zeiten als nicht-verfügbar angerechnet. Es werden daher die Variablen benötigt, die die Dauer und den Bereich des Betriebszustands (Regelbetrieb, Störungsbetrieb und Betriebsausfall) darstellen. Eine Übersicht der Qualitätsmerkmale des Bahnbetriebs und die daraus resultierenden Anforderungen sowie die benötigten Variablen für die Bewertungssystematik befindet sich in Tabelle 4.

Tabelle 4: Qualitätsmerkmale des Bahnbetriebs und die daraus resultierenden Anforderungen

Einflussfaktoren	Anforderungen	Benötigte Variable
Qualitätsmerkmale des Bahnbetriebs	Die Bewertungssystematik sollte...ermitteln können	Die Bewertungssystematik sollte die Variable...enthalten
Sicherheit	→ das Risiko des Bahnbetriebs	[Versagensrate von Technik], [Versagenswahrscheinlichkeit von Menschen], [Schadensausmaß des Versagens]
Leistungsniveau	→ das Programm des Bahnbetriebs	[Betriebsdichte], [Beförderungsgeschwindigkeit]
Verfügbarkeit	→ den Verlauf des Bahnbetriebs	[Dauer & Bereich im Regelbetrieb], [Dauer & Bereich im Störungsbetrieb/Betriebsausfall]

3.2 Das Anwendungsziel und die Anwendergruppe

Aus den Anforderungen an die Bewertungssystematik in dem letzten Abschnitt kann bereits eine Vielzahl von Variablen abgeleitet werden, die zur Bewertung von Rückfallebenenkonzepten benötigt werden. Um alle Variablen zusammenhängend in einer Bewertungssystematik berücksichtigen und die entsprechende Qualitätsaussage des Bahnbetriebs ermitteln zu können, müssen alle Variablen durch eine logische Struktur miteinander verbunden werden. Doch bevor die Struktur der Systematik entwickelt sowie der Detaillierungsgrad jeder Variable in der Systematik festgelegt werden kann, müssen das eigentliche Anwendungsziel und dessen Anwendergruppe dieser Bewertungssystematik konkretisiert werden.

Wie in Kapitel 2.3.5 bereits beschrieben, enthält ein Rückfallebenenkonzept drei Tätigkeitsfelder. Dies sind die Betriebsleitung, die Betriebsführung und die Ereignisbehandlung. Je nach der Organisationsstruktur und der Aufgabenverteilung der Bahnen können die Aufgaben eines menschlichen Akteurs sich deutlich voneinander unterscheiden. Angesichts der dynamischen Lage des IT-Angriffs sowie dessen Unberechenbarkeit bezüglich des Ausmaßes, der Dauer und der Häufigkeit hat die Anwendung dieser Bewertungssystematik im Wesentlichen das Ziel, deren Anwender bei der Entscheidungsfindung von Rückfallebenenkonzepten in der aktuellen dynamischen Betriebslage durch eine schnelle und aussagekräftige Qualitätseinschätzung zu unterstützen.

Unterschiedliche Tätigkeitsfelder eines Rückfallebenenkonzepts, wie z. B. die Betriebsleitung und die Betriebsführung, haben heute z. B. in Deutschland ein eigenes Qualitätsziel im Störungsbetrieb. Während alle Maßnahmen von der Betriebsleitung zum Erhalt des Leistungsniveaus im Vordergrund stehen, dürfen alle Maßnahmen von der Betriebsführung zur Gewährleistung der Sicherheit des Bahnbetriebs nicht unterlassen werden². Auf den ersten Blick scheint es zwischen der Betriebsleitung und der Betriebsführung einen Zielkonflikt zu geben. Wenn z. B. die Betriebsdichte oder die Größe des Störungsbereichs steigt, dann könnten sich die leistungsorientierten Maßnahmen der Betriebsleitung signifikant negativ auf die Auslastung der Menschen in der Betriebsführung auswirken und somit die Sicherheit des Bahnbetriebs gefährden. Ein solches Bedenken zum Anstieg der menschlichen Auslastung im Fall der Störung wird aber bisher weitgehend akzeptiert. In der Richtlinie „Bemessung der Arbeitsplätze“ der Deutschen Bahn zur Ermittlung des Personalbedarfs in Betriebszentralen wird beschrieben: *„Störungen und Unregelmäßigkeiten bringen im Durchschnitt nur einen geringen Zuwachs an Arbeitsbelastung. Zu der Zeit, da sie auftreten, können sie aber eine deutliche Überbelastung bewirken.“* sowie *„Weil in BZ mehrere Arbeitsplätze vereinigt sind und sich diese multifunktional nutzen lassen, können bestimmte Arbeiten delegiert werden, so dass sich ein Bediener auf die Störung konzentrieren kann.“* [81] Außerdem wurde in der

² Siehe Kapitel 2.3.5 für Details

Richtlinie erwähnt, dass in den Bemessungsfaktoren ein gewisser Umfang an Reserven berücksichtigen wurde, was allerdings in der Richtlinie nicht näher beschrieben wurde.

Das Argument in der Richtlinie aus dem Jahr 1995, dass die Störung im Durchschnitt nur einen geringen Zuwachs an Arbeitsbelastung bringe und die Überlastung in der Störung durch die Aufteilung der Arbeit zwischen den Mitarbeitern in BZ reduziert werden könne, stützt sich aber auf die Annahme, dass das herkömmliche Störungsausmaß eher klein und die Störungsdauer kurz ist. Heute nach 25 Jahren sollte dieses Argument angesichts der rasanten Entwicklung der IT und deren Anwendung im heutigen bzw. zukünftigen Bahnbetrieb neu überdacht werden. Die vollautomatisierte Betriebsabwicklung und die Passivität der Menschen im Regelbetrieb sowie die Bedrohung und die Charakteristiken eines IT-Angriffs bilden die wesentlichen Einflussfaktoren, die das vorhandene Argument im Laufe der Systementwicklung schnell widerlegen können. Aus diesem Grund ist zu erwarten, dass der Faktor Mensch in der Betriebsführung zukünftig bei der Maßnahmenfindung der Betriebsleitung mitberücksichtigt werden sollte.

Eine komplexe Bewertungssystematik mit vielen Details und Variablen bietet zwar die Möglichkeit, ein genaues und aussagekräftiges Bewertungsergebnis liefern zu können. Wenn jedoch z. B. die eigentlichen Anwender nicht über das nötige Wissen sowie über die nötigen Details über die Variablen verfügen, da die Aufgaben nicht in deren Verantwortung oder Berechtigung steht, dann bringt eine solche Komplexität keinen Nutzen für die Anwender. Angesichts des Umfangs der in Kapitel 3.1 aufgelisteten Variablen sollte die Anwendergruppe dieser Systematik die Möglichkeit haben, z. B. bei der Entscheidung der Betriebsdichte und dem Einsatz der Fdl mitwirken zu können. D. h., dass die Anwendergruppe sowohl Einfluss auf die Betriebsleitung als auch auf die Betriebsführung haben muss. In Deutschland sind die Aufgabe der Betriebsleitung und der Betriebsführung heute streng voneinander getrennt. Während einer Störung haben in Deutschland die Disponenten als Akteur der Betriebsleitung die Aufgaben, die Dispositionsmaßnahmen zu treffen und zu veranlassen. Je nach dem Ausmaß der Störung sind ggf. auch netzbezogene sowie netzübergreifende Dispositionsmaßnahmen nach Absprache mit den EVU zu erfolgen. Im Gegensatz dazu liegt die Aufgabe der Fdl und der Tf in der Betriebsführung, die Entscheidung der Disposition in einer sicheren Fahrt umzusetzen [82, 83]. Infolgedessen kann in Deutschland die Anwendung dieser Bewertungssystematik keinesfalls im Aufgabenbereich des Fdl oder des Tf liegen, da beide in der heutigen Strukturhierarchie bei der Entscheidung der Betriebsdichte bzw. der Dispositionsmaßnahmen nicht mitwirken können.

Als eine geeignete Anwendergruppe wäre nach der heutigen Organisationsstruktur des Störungsbetriebs in Deutschland (siehe Abbildung 13) z. B. der Zugdisponent. Der Zugdisponent hat heute die Aufgabe, die Konflikte zwischen Zügen der ihm zugeteilten Strecken und Knoten anhand der Dispositionsrichtlinien zu regeln. Der Zugdisponent bildet in der Organisationsstruktur die Schnittstelle zwischen Betriebsleitung und Betriebsführung und steht in direkter Verbindung zum Bereichsdisponent, von dem die netzbezogene Dispositionsmaßnahme entschieden und veranlasst wird. Außerdem hat der Zugdisponent heute

im Fall einer Störung bereits die Verantwortung, den betroffenen Bereich und die Gründe der Störung in das Dispositionsleitsystem LeiDis-NK einzutragen [82, 83]. D. h., der Zugdisponent hat nicht nur die Möglichkeit, bei der Entscheidung der Dispositionsmaßnahmen mitzuwirken, sondern verfügt er auch direkt über eine Verbindung zur unteren Strukturebene sowie über eine ausreichende Informationstiefe über die Art und das Ausmaß der Störung. Zwar hat der Zugdisponent heute keine Befugnis bei z. B. der Einsatzdauer des Fdl mitzuwirken, jedoch behindert das nicht die Anwendung der Bewertungssystematik. Z. B. können die Entscheidung über das Bewertungsergebnis und die Umsetzung der Maßnahmen dem Bezirksleiter der Betriebszentrale, der den gesamten Fahrdienst und die Betriebsführung in seiner Verantwortung hat, überlassen werden.

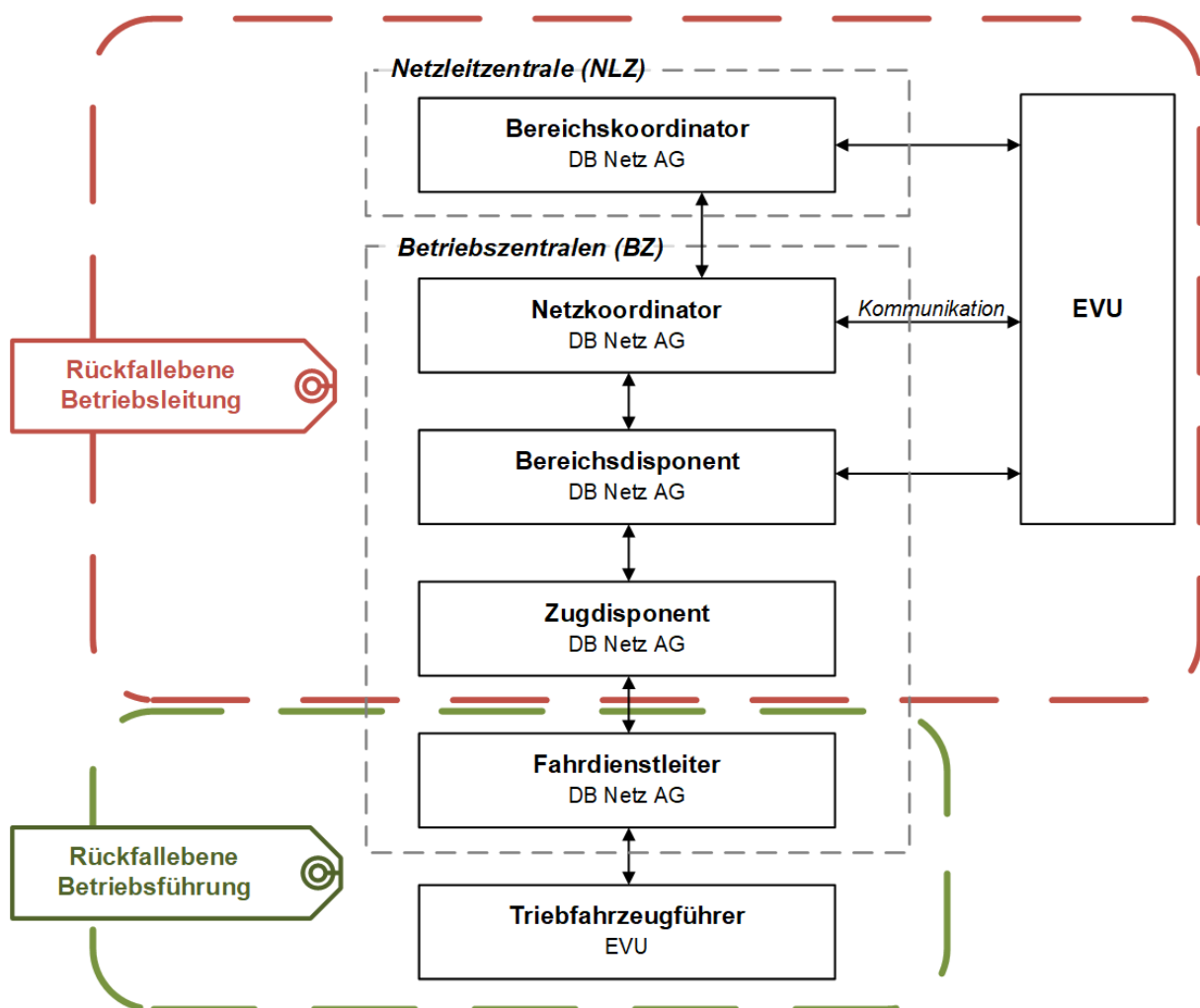


Abbildung 13: Organisationsstruktur des DB Netz AG während der Störung nach [82, 83]

3.3 Das Betriebsrisiko im Bahnbetrieb

Bei dem Strukturaufbau der Bewertungssystematik wird im Rahmen dieser Arbeit die Annahme getroffen, dass die Sicherheit des Bahnbetriebs auch bei der Berücksichtigung der Charakteristiken des IT-Angriffs stets den Vorrang vor dem Leistungsniveau und der technischen Verfügbarkeit hat. Aus diesem Grund steht die Sicherheit bzw. das Risiko im Mittelpunkt der Bewertung, während das Leistungsniveau und die technische Verfügbarkeit des Systems durch die einfachere Zusammensetzung von ausgewählten Variablen berücksichtigt werden. Daher wird in diesem Abschnitt das Betriebsrisiko bezüglich dessen Prinzip, Grenzwert sowie Anwendung ausführlich behandelt.

3.3.1 Der Kontext des Betriebsrisikos

Wie in der Durchführungsverordnung (EU) 2015/1136 zur Änderung der Durchführungsverordnung (EU) Nr. 402/2013 über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken beschrieben, ist bei der Ermittlung des Risikos des Bahnbetriebs zwischen den „*Risiken in Zusammenhang mit technischen Systemen*“, den „*betrieblichen Risiken*“ und den „*Gesamtrisiken auf der Ebene des Eisenbahnsystems*“ zu unterscheiden [84]. Das Betriebsrisiko im Rahmen dieser Bewertungssystematik stützt sich auf das Konzept der „*betrieblichen Risiken*“. Die Verordnung empfiehlt zwar eine Differenzierung zwischen den drei Risikoaspekten, liefert aber keine nähere Beschreibung zum Unterschied zwischen den Risikoaspekten. Um die Sicherheit des Bahnbetriebs in der vorliegenden Arbeit verstehen zu können, muss das Konzept des Betriebsrisikos im Rahmen dieser Bewertungssystematik im Vorfeld definiert werden. Das Betriebsrisiko muss von den Risiken mit technischen Systemen sowie von dem Gesamtrisiko auf der Ebene des Eisenbahnsystems unterschieden werden. Im folgenden Abschnitt wird zur Differenzierung der Risikoaspekte das Risiko in Zusammenhang mit technischen Systemen als „technisches Risiko“, das betriebliche Risiko als „Betriebsrisiko“ und das Gesamtrisiko auf der Ebene des Eisenbahnsystems als „Gesamtrisiko“ bezeichnet.

Nach der Richtlinie (EU) 2016/797 über die Interoperabilität des Eisenbahnsystems enthält ein Eisenbahnsystem strukturelle und funktionelle Teilsysteme. Bei den strukturellen Teilsystemen handelt es sich um die Infrastruktur, die Energie, die Zugsteuerung/Zugsicherung, die Signalgebung und das Fahrzeug. Bei den funktionellen Teilsystemen handelt es sich um die Bereiche Betriebsführung, Verkehrssteuerung, Instandhaltung sowie die Telematikanwendungen für den Personen- und Güterverkehr. Dadurch lässt sich annehmen, dass bei der Ermittlung des Gesamtrisikos alle Teilsysteme umfassend berücksichtigt werden müssen. Das bedeutet, dass neben den üblichen Risiken, die aus der Zuverlässigkeit der strukturellen Teilsystemen resultieren, auch alle Verfahren der funktionellen Teilsysteme sowie die Menschen berücksichtigt werden müssen, einschließlich des Risikos des Störungsbetriebs und der Instandhaltung.

Im Vergleich zum Gesamtrisiko werden bei der Ermittlung des technischen Risikos lediglich bestimmte technische Systeme in den strukturellen Teilsystemen berücksichtigt. Daher fällt die Infrastruktur aus dem Umfang der Risikobetrachtung heraus. Zusätzlich sind die Menschen und deren Handlungen sowie der Instandhaltungsprozess nach der Definition der Durchführungsverordnung (EU) Nr. 402/2013 kein Bestandteil eines technischen Systems [20]. Dadurch wird das Risiko der menschlichen Faktoren sowie der Instandhaltung bei der Ermittlung des technischen Risikos ebenfalls explizit ausgeschlossen. Anders als das Gesamtrisiko, in dem auch das Risiko des Störungsbetriebs berücksichtigt wird, befasst sich das technische Risiko lediglich mit dem Regelbetrieb. Im Fall einer Störung soll das technische System den Bahnbetrieb zu einem sicheren Zustand führen. Die weitere Betriebsführung im Störungsbetrieb mit der Teilnahme der Menschen fällt dann nicht mehr allein in den Zuständigkeitsbereich des technischen Systems.

Im Vergleich zum Gesamtrisiko und zum technischen Risiko fällt das Betriebsrisiko im Kontext der vorliegenden Bewertungssystematik zwischen den Kontext des Gesamtrisikos und des technischen Risikos. Ähnlich wie bei dem Gesamtrisiko werden beim Betriebsrisiko sowohl die Risiken der technischen Systeme als auch die Risiken der Menschen und deren Handlungsprozesse berücksichtigt. Außerdem umfasst das Betriebsrisiko nicht nur das Risiko im Regelbetrieb, sondern auch das Risiko im Störungsbetrieb, der im Wesentlichen in der Verantwortung der Menschen liegt. Allerdings enthält das Betriebsrisiko genau wie das technische Risiko keine Risiken der Infrastruktur und des Instandhaltungsprozesses. Anders als der Zweck der Ermittlung des technischen Risikos, die außer der Risikoermittlung auch zur Ableitung von Sicherheitsanforderungen an das betrachtete System angewendet wird, dient die Ermittlung des Betriebsrisikos im Rahmen dieser Arbeit als eine schnelle Entscheidungshilfe für die Gestaltung von Rückfallebenenkonzepten im Bahnbetrieb. Zusätzlich unterscheiden sich das technische Risiko und das Betriebsrisiko im Konzept dieser Arbeit in folgenden Punkten: der Zeitpunkt und der Zeitbedarf, der Umfang der betrachteten Betriebsfunktionen, der Zeitraum und der Bereich der Betrachtung, die Art des Betriebsprogramms und der Netzstruktur sowie die Verbindlichkeit des Risikogrenzwerts.

Eine Zusammenfassung der Unterschiede zwischen dem technischen Risiko und dem Betriebsrisiko befindet sich in Tabelle 5. Die Unterschiede der einzelnen Punkte sind wie folgt:

Der Zeitpunkt der Ermittlung des technischen Risikos erfolgt im Grunde während des Entwicklungsprozesses des technischen Systems. Nach den Phasen der Lebenszyklen in EN 50126-1 [27] kann z. B. während der Phase der Risikoanalyse zur Ableitung der Sicherheitsanforderung an das technische System angewendet werden oder nach der Zuteilung der Anforderungen an das System im Rahmen der System Entwicklung zur Ermittlung vom technischen Risiko des technischen Systems. Die Ermittlung des technischen Risikos wird in der Regel mit einer Referenznetzstruktur sowie einem Musterbetriebsprogramm durchgeführt. Gründe dafür können z. B. die Reduzierung des Analyseaufwands oder das Fehlen einer Struktur und der Betriebsdetails während des Entwicklungsprozesses sein. Das Ergebnis der Analyse gilt dann für alle vergleichbaren Netzbereiche mit einem ähnlichen Betriebsprogramm.

Für eine solche Analyse stehen meistens je nach Entwicklungsprozess mehrere Monate oder mehrere Jahre zur Verfügung. Eine dynamische Anpassung des Ergebnisses während des laufenden Betriebs ist nicht vorgesehen. Während der Analyse wird / werden ausschließlich die Betriebsfunktion(en) im Bahnbetrieb betrachtet, die dem betrachteten technischen System zugehörig ist / sind. Der Zeitraum der Betrachtung beträgt meistens eine Betriebsstunde des betrachteten technischen Systems, z. B. eine Stunde Zugfahrt. Der Risikogrenzwert des technischen Risikos ist in Europa z. B. durch die EU Verordnung über die Gemeinsame Sicherheitsmethode (CSM) in [20, 84] geregelt. Zur Beurteilung des ermittelten technischen Risikos eines betrachteten technischen Systems muss ein ausgewählter Risikogrenzwert herangezogen werden. Das ermittelte technische Risiko eines gefährlichen Funktionsversagens des betrachteten technischen Systems darf dann die Vorgabe des ausgewählten Risikogrenzwerts nicht überschreiten.

Im Gegensatz zum technischen Risiko erfolgt die Ermittlung des Betriebsrisikos im Konzept dieser Arbeit durchgehend im laufenden Betrieb, insbesondere im Fall einer Störung. Die Analyse dient zu einer schnellen Entscheidungshilfe von Rückfallebenenkonzepten. Für die Ermittlung des Betriebsrisikos steht daher vergleichsweise nur eine kurze Zeit zur Verfügung, z. B. mehrere Stunden bis zu einem Tag. Außerdem muss das Ergebnis nach der aktuellen Lage der Störung während des Bahnbetriebs dynamisch angepasst werden. Daher wird die Ermittlung des Betriebsrisikos mit der tatsächlichen Netzstruktur und dem ortsspezifischen Betriebsszenario durchgeführt. Das Ergebnis der Analyse ist dann nur für diesen Betrachtungsbereich sowie das vorliegende Betriebsszenario gültig. Während der Analyse des Betriebsrisikos werden alle Betriebsfunktionen betrachtet, die für die Realisierung des Bahnbetriebs bzw. für die sichere Durchführung einer Fahrt notwendig sind. Da der Risikogrenzwert des Betriebsrisikos sowie dessen Ergebnisinterpretation bisher ungeregelt sind, werden die beiden Themen in den nächsten Kapiteln 3.3.2 und 3.3.3 ausführlich behandelt und die Lösungsansätze ausgearbeitet.

Tabelle 5: Vergleich von technischem Risiko und Betriebsrisiko.

	Ermittlung des technischen Risikos	Ermittlung des Betriebsrisikos
Kontext des Risikos	Es wird nur das Risiko eines betrachteten technischen Systems im Regelbetrieb berücksichtigt. Das Risiko im Störungsbetrieb wird nicht betrachtet.	Es wird das Betriebsrisiko des Bahnbetriebs berücksichtigt, sowohl das Risiko im Regelbetrieb als auch das Risiko im Störungsbetrieb.
Zeitpunkt und Zeitbedarf der Ermittlung	Während des Entwicklungsprozesses, insbesondere in der Phase der Lebenszyklen Risikoanalyse und Entwicklung. Die Analyse dient zu einer detaillierten Risikobetrachtung des technischen Systems. Für die Analyse stehen meistens Monate oder Jahre zur Verfügung. Eine dynamische Anpassung des Ergebnisses während des Betriebs ist nicht vorgesehen.	Durchgehend im laufenden Betrieb, insbesondere im Fall der Störung. Die Analyse dient zur schnellen Entscheidungshilfe des Rückfallebenenkonzepts. Für die Analyse steht im Vergleich dazu nur eine kurze Zeit zur Verfügung und deren Ergebnis muss nach der Lage der Störung dynamisch angepasst werden.
Zweck der Ermittlung	Ermittlung des technischen Risikos oder auch zur Ableitung von Sicherheitsanforderungen eines betrachteten technischen Systems	Zur Gestaltung des Betriebskonzepts und des Rückfallebenenkonzepts im Bahnbetrieb
Umfang der betrachteten Betriebsfunktionen	Es wird nur die Betriebsfunktion betrachtet, die dem betrachteten technischen System zugehörig sind	Es werden alle Betriebsfunktionen betrachtet, die für die Realisierung des Bahnbetriebs bzw. für die Durchführung einer sicheren Fahrt notwendig sind
Umfang der betrachteten Systemakteure	Es werden nur die technischen Systeme betrachtet. Die Infrastruktur, der Mensch und deren Handlungen sowie der Instandhaltungsprozess sind nicht Bestandteil der Betrachtung.	Es werden alle Akteure des Bahnbetriebs betrachtet, sowohl die technischen Systeme als auch die menschlichen Akteure und deren Handlungsprozesse, jedoch ohne die bauliche Infrastruktur, Energie und den Instandhaltungsprozess.
Art des Betriebsprogramms und Netzstruktur	Die Analyse wird meist mit einer Referenznetzstruktur und einem Musterbetriebsprogramm durchgeführt. Das Ergebnis der Analyse gilt dann für alle vergleichbaren Netzbereiche.	Die Analyse wird mit der tatsächlichen Netzstruktur und dem ortsspezifischen Betriebsszenario durchgeführt. Das Ergebnis ist nur für den Betrachtungsbereich unter dem vorgegebenen Betriebsszenario gültig.
Zeitraum und Bereich der Risikobetrachtung	Es wird nur das Risiko des Bahnbetriebs mit dem betrachteten technischen System für z. B. eine Betriebsstunde auf der Referenznetzstruktur berechnet.	Es wird das Betriebsrisiko des Bahnbetriebs mit allen Akteuren in dem betrachteten Netzbereich über den Betrachtungszeitraum berechnet.
Risikogrenzwert	Der Risikogrenzwert ist in Europa weitgehend z. B. durch die CSM Verordnung geregelt.	Der Risikogrenzwert ist bisher ungeregelt bzw. unbekannt.

3.3.2 Der Risikogrenzwert des Betriebsrisikos

Der Risikogrenzwert ist nach [20] ein Bezugskriterium, um die Akzeptanz eines spezifischen Risikos zu beurteilen. Wie in Kapitel 3.3.1 bereits beschrieben, kann der Risikogrenzwert des technischen Risikos in Europa aus den Anforderungen der Durchführungsverordnung über die gemeinsame Sicherheitsmethode abgeleitet werden. In der Durchführungsverordnung 402/2013 wurde der Risikogrenzwert für technische Systeme (RAC-TS) wie folgt festgelegt:

„Bei technischen Systemen, bei denen im Falle eines funktionellen Ausfalls von unmittelbaren katastrophalen Folgen auszugehen ist, muss das damit verbundene Risiko nicht weiter reduziert werden, wenn die Ausfallrate pro Betriebsstunde kleiner oder gleich $1E-09$ ist.“[20] Um den Risikogrenzwert ableiten zu können, sind nach der Definition des Risikos die Versagensrate des technischen Systems sowie das Schadensausmaß des Versagens notwendig. Aus den vorliegenden Anforderungen lässt sich zwar die zulässige Versagensrate des technischen Systems von $1E-09$ Versagen/Betriebsstunde bei einem Versagen mit einer katastrophalen Folge direkt ablesen, jedoch wurde das Ausmaß dieser katastrophalen Folge in der Verordnung nicht näher beschrieben. Um die in der Verordnung definierten Anforderungen an die technischen Systeme anwenden zu können, wurde z. B. die Methode Risk Score Matrix (RSM) entwickelt. Die RSM ist eine Methode zur Ableitung der Sicherheitsanforderungen an die technischen Systemen, die spezifisch auf die Anforderungen der CSM-Verordnung kalibriert ist [85, 86].

Wie in Abbildung 14 dargestellt wird, enthält die RSM eine Kombination aus 10 Stufen Sicherheitsanforderungen und 7 Stufen Unfallklassen.

Sicherheitsanforderung 1/h	Risk Score Matrix						
keine							
10^{-5}							
3×10^{-6}							
10^{-6}							
3×10^{-7}							
10^{-7}							
3×10^{-8}							
10^{-8}							
3×10^{-9}							
10^{-9}							
	A	B	C	D	E	F	G
	Unfallklasse						

Abbildung 14: Aufbau der Risk Score Matrix in VDE V 0831-103 [85]

Durch die Kombination von Unfallklassen und Sicherheitsanforderungen ergibt sich das technische Risiko des betrachteten technischen Systems. Der Risikogrenzwert ist implizit in der RSM enthalten. Dadurch ist die RSM in zwei Bereiche aufgeteilt. Die technischen Risiken in dem grau markierten Zellenbereich sind nicht zulässig bzw. nicht akzeptabel. D. h., solange die Kombination aus der Sicherheitsanforderung und der Unfallklasse sich in dem weiß markierten Zellenbereich befindet, ist das technische Risiko des technischen Systems akzeptabel. Beispielsweise darf bei einem Versagen des technischen Systems mit dem höchsten Schadensausmaß in der Unfallklasse G die Sicherheitsanforderung bzw. die Versagensrate des

technischen Systems nur höchstens $1\text{E-}09$ Versagen/Betriebsstunde betragen. Dadurch lässt sich der Risikogrenzwert in der RSM an der Grenze zwischen den weißen und den grau markierten Zellen als Produkt der beiden Werte bestimmen.

Der Risikogrenzwert in der RSM basiert auf der Annahme einer konstanten Kritikalität des Risikos [87]. Nach dieser Annahme sollte der Risikogrenzwert bei allen Unfallklassen identisch sein. Dadurch reduziert sich die Sicherheitsanforderung an das technische System bzw. steigt die Versagensrate des technischen Systems mit der sinkenden Unfallklasse bzw. dem sinkenden Schadensausmaß. Das Schadensausmaß der Unfallklasse bezüglich des Personenschadens wird in der RSM durch die Stufen der Verletzung und die Anzahl der Betroffenen voneinander differenziert. Es gibt vier Stufen der Verletzung: keine Verletzte, Leichtverletzte, Schwerverletzte und Getötete. Nach dem Statistischen Bundesamt [88] werden die Stufen der Verletzung wie folgt definiert:

- Getötete: „Personen, die innerhalb von 30 Tagen an den Unfallfolgen starben“
- Schwerverletzte: „Personen, die unmittelbar zur stationären Behandlung (mindestens 24 Stunden) in einem Krankenhaus aufgenommen wurden“
- Leichtverletzte: „Alle übrigen Verletzten“

Die Anzahl der Betroffenen wurde semi-qualitativ durch „ein“, „mehrere“ und „viele“ beschrieben, wobei „mehrere“ im Sinne von „ca. 3“ und „viele“ im Sinne von „ca. 10“ zu verstehen sind [85]. Nach [87] lässt sich die Anzahl der Opfer in den unterschiedlichen Stufen der Verletzung anhand der folgenden Heuristik auf eine gleiche Einheit (Opfer) zusammenfassen:

$$\text{Anzahl Opfer} = \text{Getötete} + \text{Anzahl Schwerverletzte} / 10 + \text{Anzahl Leichtverletzte} / 100 \quad (1)$$

Dadurch lässt sich die Opferzahl der Unfallklasse in der RSM anhand der Heuristik ausrechnen, wie in Tabelle 6 gezeigt wird. Durch die Kombination aus Unfallklassen (z. B. 3 Opfer/Versagen bei Unfallklasse G) und zulässigen Sicherheitsanforderungen (z. B. $1\text{E-}09$ Versagen/Betriebsstunde bei Unfallklasse G) ergibt sich nach dem Konzept der RSM ein konstanter Risikogrenzwert von $3\text{E-}09$ Opfer/Betriebsstunde.

Tabelle 6: Unfallklasse der RSM und deren Anzahl Opfer nach der Umrechnung

Unfallklasse	Schadensausmaß	Anzahl Opfer
A	Keine Verletzten	0
B	Ein Leichtverletzter	0,01
C	Mehrere Leichtverletzte	0,03
D	Ein Schwerverletzter oder viele Leichtverletzte	0,1
E	Mehrere Schwerverletzte	0,3
F	Ein Todesfall oder viele Schwerverletzte	1
G	Mehrere Todesfälle	3

Es ist durchaus bekannt, dass das Betriebsrisiko eines menschlichen Versagens in der Rückfallebene im Fall einer technischen Störung signifikant höher als das Betriebsrisiko im technischen gesicherten und automatisierten Regelbetrieb ist [89]. Es stellt sich an dieser Stelle die Frage, ob es in dem Risikogrenzwert des technischen Systems noch ausreichende Risikoreserve gibt, um auch die menschlichen Risiken im Störungsbetrieb einschließen zu können. Um die Frage beantworten zu können, wird hier das Betriebsrisiko des Schienenverkehrs in Deutschland vereinfacht eingeschätzt und dessen Ergebnis mit der Unfallstatistik des Statistischen Bundesamts verglichen. Aufgrund der fehlenden Daten der genauen Ausfallrate soll die folgende Berechnung nur beispielhaft zeigen, wie der Ansatz zum Vergleich des Risikogrenzwerts anzuwenden ist.

Grundsätzlich sind in dem Ergebnis des Betriebsrisikos sowohl die Risiken des Regelbetriebs als auch die Risiken des Störungsbetriebs im Gesamtzeitraum der Risikobetrachtung enthalten. Wenn angenommen wird, dass der Bahnbetrieb im Gesamtzeitraum der Risikobetrachtung durchgehend in einem technischen gesicherten und automatisierten Regelbetrieb durchgeführt wird, dann enthält das Ergebnis des Betriebsrisikos lediglich die Risiken der technischen Systeme. Da die Risiken der Infrastruktur und der Energie nicht im Kontext des Betriebsrisikos enthalten sind, bleiben nach Abbildung 5 lediglich die Leit- und Sicherungstechnik und das Fahrzeug als technische Systeme, die für die Realisierung einer Fahrt notwendig sind. Die Funktion der Leittechnik dient zur optimalen Ablaufsteuerung der Haupt- und Nebenprozesse in einem Verkehrssystem, wie z. B. in der Disposition, die aber in der Regel nicht sicherheitsrelevant ist [42, 90]. Dadurch bleibt nur die Sicherungstechnik und Fahrzeug als maßgebliche Akteure für eine sichere Durchführung der Fahrt in einem technischen gesicherten Regelbetrieb. Während die Sicherungstechnik nach den generischen Aufgaben der Betriebsführung (siehe Abbildung 9) die Betriebsfunktion „Fahrten sichern“ hat, ist das Fahrzeug in dieser vereinfachten Analyse für die Betriebsfunktion „Fahrten durchführen“ zuständig. Die Ausfallrate eines technischen Systems pro Betriebsstunde, bei dem im Fall eines funktionellen Ausfalls von unmittelbaren katastrophalen Folgen auszugehen ist, darf nach der CSM-Verordnung nicht kleiner als $1\text{E-}09$ sein [20]. Allerdings schreibt die CSM-Verordnung nicht vor, wie genau diese Anforderung anzuwenden ist. Dadurch entsteht bei der Umsetzung dieser Anforderung ein Interpretationsspielraum [91]. Es wird daher angenommen, dass die Sicherungstechnik und das Fahrzeug durch den Trend der Miniaturisierung sowie der Virtualisierung künftig jeweils als einzelnes technisches System betrachtet werden können. Außerdem sind die Sicherungstechnik und das Fahrzeug zwei komplett unabhängige technische Systeme. Der Risikogrenzwert der Sicherungstechnik sowie des Fahrzeugs in Höhe von $3\text{E-}09$ Opfer/Betriebsstunde ergibt sich dann nach der RSM aus dem Produkt der Ausfallrate eines technischen Systems in Höhe von $1\text{E-}09$ Ausfall/Betriebsstunde und der Unfallklasse einer katastrophalen Folge mit 3 Opfern/Ausfall, wie in Abbildung 14 dargestellt ist. Dadurch lässt sich der Risikogrenzwert eines technischen gesicherten Regelbetriebs pro Betriebsstunde ($6\text{E-}09$ Opfer/Betriebsstunde) aus der Summe des Risikogrenzwerts der Sicherungstechnik

(3E-09 Opfer/Betriebsstunde) und des Risikogrenzwerts des Fahrzeugs (3E-09 Opfer/Betriebsstunde) zusammenrechnen.

Das Konzept des Betriebsrisikos hat im Rahmen dieser Arbeit das Ziel, die folgende Frage zu beantworten: „Wird der Bahnbetrieb unter der Zusammensetzung von bestimmten Akteuren in einem bestimmten Bereich über einem bestimmten Zeitraum mit einem bestimmten Betriebsprogramm ausgeführt, wie viele Opfer werden am Ende des Gesamtzeitraums erwartet?“ Um die erwartete Opferzahl im Gesamtzeitraum der Risikobetrachtung und dem Ergebnis der Unfallstatistik vergleichen zu können, wird der Risikogrenzwert des technischen gesicherten Regelbetriebs pro Betriebsstunde auf ein Kalenderjahr hochgerechnet. Die Betriebsstunde hier ist aber keine Realstunde, sondern die Betriebsstunde eines technischen Systems. Das bedeutet, falls sich in einem bestimmten Bereich mehrere identische technische Systeme im Betrieb befinden, z. B. mehrere Fahrzeuge, dann müssen bei der Ermittlung des Betriebsrisikos die Betriebsrisiken aller Fahrzeuge im gesamten Zeitraum der Betrachtung berücksichtigt werden. Die Summe der gesamten Betriebsstunden wird hier näherungsweise durch die Summe der gesamten Reisezeiten aller Fahrten im gesamten Zeitraum und Bereich der Betrachtung dargestellt. Die Summe der gesamten Reisezeiten aller Fahrten kann z. B. durch die gesamte Betriebsleistung im Gesamtzeitraum der Betrachtung, geteilt durch die mittlere Beförderungsgeschwindigkeit aller Fahrten, näherungsweise eingeschätzt werden.

Wie in Tabelle 7 gezeigt wird, beträgt die Verkehrsleistung des Schienenverkehrs in Deutschland im Zeitraum von 2006 bis 2017 im Durchschnitt 1.321 Mio. Zugkilometer (Zkm) im Jahr. Darunter sind 144 Mio. Zkm des SPFV, 946 Mio. Zkm des SPNV und 231 Mio. Zkm des Schienengüterverkehrs (SGV). Die mittlere Beförderungsgeschwindigkeit wird nach Anhang A im SPFV mit 140 km/h, im SPNV mit 70 km/h und im SGV mit 50 km/h angenommen. Dadurch lassen sich die gesamten Reisezeiten der einzelnen Segmente entsprechend Tabelle 7, Zeile Nr. (3) ausrechnen. Der Risikogrenzwert des Bahnbetriebs unterscheidet sich an dieser Stelle nicht zwischen dem SPFV, dem SPNV und dem SGV, da die Risikokritikalität nach dem Konzept der RSM bei allen Unfallklassen konstant und daher identisch ist. Letztendlich lässt sich der Grenzwert des Betriebsrisikos eines technisch gesicherten Bahnbetriebs pro Jahr in Deutschland nach dieser vereinfachten Rechnung auf 0,12 Opfer/Jahr einschätzen.

Falls der hier ermittelte Risikogrenzwert von 0,12 Opfer/Jahr als ein allgemeiner Risikogrenzwert für das Betriebsrisiko übernommen werden könnte, müsste in diesem Risikogrenzwert auch eine ausreichende Reserve vorhanden sein, um die zusätzlichen Risiken der menschlichen Akteure im Störungsbetrieb einschließen zu können. Betrieblich bedeutet das, dass die Summe der Opfer aus allen Eisenbahnunfällen in Deutschland, sowohl Unfälle im Regelbetrieb als auch im Störungsbetrieb, sowie Unfälle aufgrund technischen Versagens und aufgrund menschlichen Versagens, in einem Gesamtzeitraum von einem Jahr den Risikogrenzwert 0,12 Opfer/Jahr nicht überschreiten sollte.

Tabelle 7: Vereinfachte Risikoschätzung des Betriebsrisikos bei einem technisch gesicherten Regelbetrieb für Schienenverkehr in Deutschland

Nr.	Parameter	Einheit	SPFV	SPNV	SGV
(1)	Mittlere Zugkilometer im Jahr (2006 – 2017) ¹	Zkm ² /Jahr	144 Mio.	946 Mio.	231 Mio.
(2)	Mittlere Beförderungsgeschwindigkeit ³	km/h	140 km/h	70 km/h	50 km/h
(3)	Gesamte Reisezeiten im Jahr = (1)/(2)	Std./Jahr	1.028.571	13.514.286	5.775.000
(4)	Risikogrenzwert pro Std. = (4-1)+(4-2)		6E-09	6E-09	6E-09
	(4-1) Risikogrenzwert Sicherungstechnik	Opfer/Std.	3E-09	3E-09	3E-09
	(4-2) Risikogrenzwert Fahrzeug	Opfer/Std.	3E-09	3E-09	3E-09
(5)	Risikogrenzwert im Jahr = (3)*(4)	Opfer/Jahr	0,01	0,08	0,03
Risikogrenzwert des technischen gesicherten Bahnbetriebs			0,12 Opfer/Jahr		

1. nach dem Statistischen Bundesamt [92, 93]

2. Zugkilometer (Zkm): zurückgelegte Kilometerstrecke der Züge

3. siehe Anhang A

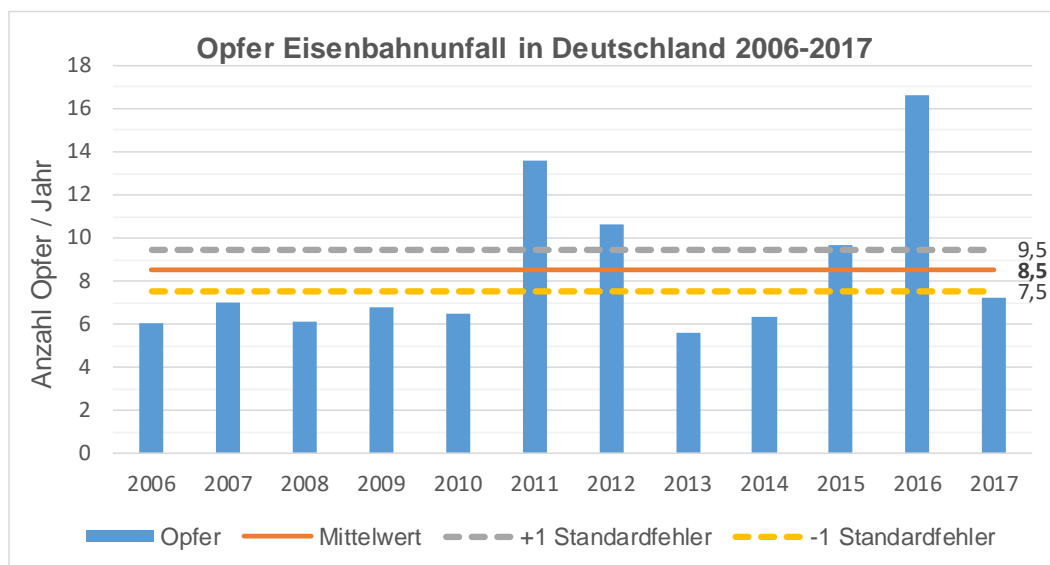
Zum Vergleich des Risikogrenzwerts wird hier die Eisenbahnunfallstatistik des Statistischen Bundesamts im Zeitraum von 2006 bis 2017 herangezogen. Aus den unterschiedlichen Unfallarten wurden zum Vergleich nur die folgenden vier Unfallarten berücksichtigt, nämlich die Entgleisung, der Zusammenstoß, der Aufprall auf Gegenstände und der Zusammenprall mit Wegebenutzern³. Außerdem wurden bei den Opfern lediglich die Personengruppen berücksichtigt, die sich während des laufenden Betriebs im Zug befinden. Dies sind die Reisenden sowie die Bahnbediensteten. Um das Ergebnis der Unfallstatistik mit dem Risikogrenzwert vergleichen zu können, wurde die Anzahl der Personen, die bei einem Unfall verletzt oder getötet wurde, durch die Formel (1) auf eine gleiche Einheit (Opfer) umgerechnet. Da in der Unfallstatistik bei den verletzten Personen nicht zwischen den Schwerverletzten und den Leichtverletzten unterschieden wurde, ist die Anwendung der Umrechnungsheuristik auf die Daten des Statistischen Bundesamts nicht möglich. An dieser Stelle wurde zur Umrechnung der Opferzahlen die folgende Heuristik nach [94] herangezogen:

$$\text{Anzahl Opfer} = \text{Getötete} + \text{Anzahl Verletzte} / 50 \quad (2)$$

Wie die Ergebnisse der Umrechnung in Tabelle 8 zeigen, liegt die Anzahl Opfer im Eisenbahnverkehr im Zeitraum von 2006 bis 2017 zwischen 5,6 Opfern und 16,6 Opfern im Jahr. Der Durchschnitt liegt bei 8,5 Opfer/Jahr mit einem Standardfehler von $\pm 1,0$ Opfer/Jahr.

³ Details über die vier Unfallarten siehe Kapitel 3.4.2.5

Tabelle 8: Anzahl Opfer Eisenbahnunfall in Deutschland von 2006 bis 2017 nach [92, 93]



Jahr	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Getötete	0	2	2	2	1	10	6	1	1	5	12	2
Verletzte	302	252	206	239	273	178	230	232	268	232	231	262
Opfer	6,0	7,0	6,1	6,8	6,5	13,6	10,6	5,6	6,4	9,6	16,6	7,2
Mittelwert	8,5 [Opfer/Jahr]											

Durch den Vergleich mit der Unfallstatistik wird gezeigt, dass die tatsächliche Opferzahl des Bahnbetriebs nach der Statistik mit 8,5 Opfer/Jahr deutlich höher als der Risikogrenzwert eines technischen gesicherten Regelbetriebs mit 0,12 Opfer/Jahr ist. Es lässt sich zwar darüber diskutieren, ob die Annahme in der vorliegenden vereinfachten Berechnung, in der nur zwei technische Systeme betrachtet wurden, der heutigen Systemauslegung entspricht, da das heutige System Bahn aus mehreren technischen Systemen besteht. Aber auch, wenn das Ergebnis des Risikogrenzwerts eines technisch gesicherten Regelbetriebs um den Faktor 10 erhöht wird, was hier bedeutet, dass das System Bahn aus 10 technischen Systemen mit der höchsten Sicherheitsanforderung besteht, liegt der neue Risikogrenzwert in Höhe von 1,2 Opfern/Jahr weiterhin deutlich unter dem Ergebnis der statistischen Daten von 8,5 Opfern/Jahr. Daher kann die Schlussfolgerung gezogen werden, dass der Risikogrenzwert aus einem technisch gesicherten Regelbetrieb keine ausreichende Risikoreserve enthält, um die Risiken der menschlichen Akteure im Störungsbetrieb einschließen zu können. Das bedeutet auch, dass der Risikogrenzwert des Betriebsrisikos neu festgelegt werden muss. Hier muss aber beachtet werden, dass die Sicherheitsanforderung an das technische System sowie der Risikogrenzwert des technischen Risikos trotz der Erhöhung des Risikogrenzwerts des Betriebsrisikos unverändert bleiben muss. Die Sicherheitsanforderung an das technische System wurde rechtlich festgelegt und bietet bisher auch eine ausreichende Sicherheit im technisch gesicherten Regelbetrieb. Die Erhöhung und die neue Festlegung des Risikogrenzwerts des Betriebsrisikos hat nur den Zweck, durch eine annehmbare Risikoreserve die Risiken des Störungsbetriebs in der menschlichen Verantwortung sowie die Risiken der unberechenbaren IT-Angriffsbedrohung einschließen zu können.

Da bisher weder in der Normung noch in den Gesetzen eine Vorgabe zum Risikogrenzwert des Betriebsrisikos zu finden ist, wird der Risikogrenzwert im Rahmen dieser Arbeit aus der Unfallstatistik des öffentlichen Schienennetzes in Deutschland abgeleitet⁴. Ein ähnliches Vorgehen ist auch in der EN 50126-2, Anhang B zu finden. Dort werden die Unfallstatistiken angewendet, um die tolerierbare Gefährdungsrate (THR) ohne präzise erfasste Modelle zu ermitteln [22]. Es ist zu beachten, dass es sich bei der in dieser Arbeit aus der Unfallstatistik abgeleiteten Opferzahl von 8,5 Opfern/Jahr um einen Mittelwert im öffentlichen Schienenverkehrsnetz in Deutschland handelt. Nach dem Streckenstandard der DB Netz AG hat jedoch jeder Streckenstandard eine unterschiedliche planerische Betriebsdichte und Betriebsgeschwindigkeit. Dies bedeutet auch, dass das Betriebsrisiko bei jedem Streckenstandard unterschiedlich sein kann. Unter einer gleichen Betriebsdichte hat der Streckenstandard mit einer höheren Geschwindigkeit im Gegensatz zum Streckenstandard mit einer niedrigen Geschwindigkeit auch ein höheres Betriebsrisiko. Dies hat zur Folge, dass die mittlere Opferzahl aus der Unfallstatistik nicht unbedingt der zu erwarteten Opferzahl bzw. dem zu erwarteten Betriebsrisiko des betrachteten Streckenstandards entspricht. Aus diesem Grund wird die mittlere Opferzahl in dieser Arbeit dem Betriebsrisiko des Streckenstandards und dem Anteil des Streckenstandards im Gesamtnetz angepasst.

Zur Ermittlung des stündlichen Betriebsrisikos des Streckenstandards im Regelbetrieb werden zunächst die mittlere Betriebsdichte und die mittlere Beförderungsgeschwindigkeit für jeden Streckenstandard festgelegt. Anschließend wird das Schadensausmaß durch die Kombination von Unfallvariablen für jeden Streckenstandard eingeschätzt. Die Bestimmung des stündlichen Betriebsrisikos erfolgt durch die Anwendung der Bewertungssystematik, die in Kapitel 3 ausführlich behandelt wird. Die Höhe der Anpassung eines Streckenstandards s lässt sich durch den Quotient des stündlichen Betriebsrisikos des Streckenstandards s (SBR_{Rs}) und der Summe aller Produkte des stündlichen Betriebsrisikos des Streckenstandards s (SBR_{Rs}) und dessen Anteil der Gleislänge im Gesamtnetz (GL_{As}) bestimmen, wie die Formel (3) zeigt:

$$RG_{As} = RG_M * \frac{SBR_{Rs}}{\sum_{s=1}^m (SBR_{Rs} * GL_{As})} \quad (3)$$

- RG_{As} : Der angepasste Risikogrenzwert pro Kalenderjahr des Streckenstandards s
 RG_M : Der Risikogrenzwert (Mittlere Opferzahl) pro Kalenderjahr aus der Unfallstatistik
 SBR_{Rs} : Das stündliche Betriebsrisiko im Regelbetrieb des Streckenstandards s
 GL_{As} : Anteil der Gleislänge des Streckenstandards s im Gesamtnetz
bei $s = 1$: Der erste Typ des Streckenstandards im Gesamtnetz
bei $s = m$: Der letzte Typ des Streckenstandards im Gesamtnetz

⁴ Das Betriebsrisiko beinhaltet nach dem Konzept der vorliegenden Arbeit keine Risiken der baulichen Infrastruktur. Da die Opferzahl in der Unfallstatistik nicht nach Ursachen (Technisches System, Menschen oder Infrastruktur) unterschieden wird, wird angenommen, dass die Opferzahl, deren Ursache auf die bauliche Infrastruktur zurückzuführen ist, sehr gering ist. Dies wird damit begründet, dass auch die Störbestehenszeiten der baulichen Infrastruktur im Bereich des DB Netz AG lediglich einen geringen Anteil von 4,28% an den gesamten Störbestehenszeiten haben, wie in Tabelle 11 gezeigt wird.

Nach dem Ergebnis in Tabelle 9 beträgt im vorliegenden Rechenbeispiel der Risikogrenzwert des Streckenstandard M160 nach der Anpassung 14,37 Opfer/Jahr. Es muss beachtet werden, dass sich der angepasste Risikogrenzwert des Streckenstandards M 160 von 14,37 Opfern/Jahr nicht auf dessen Gleislänge bezieht, sondern auf die gesamte Gleislänge im öffentlichen Schienennetz. Dies hat die folgende Bedeutung: Falls alle Strecken des öffentlichen Schienennetzes den gleichen Streckenstandard M 160 haben, wird bei dem Bahnbetrieb auf dem gesamten öffentlichen Schienennetz eine Opferzahl von 14,37 Opfern/Jahr erwartet.

Tabelle 9: Anpassung des Risikogrenzwerts nach Risiko und Anteil des Streckenstandards.

Strecken- standard	D _{AR}	V _B	Unfallart	Unfallkom- bination	Unfall- geschwindigkeit	S	BR _R	GL _A	RG _A
P 300	10	170	Zusammenstoß	GZ-RZ / RZ-RZ	V > 160	30	1,88E-07	3,46%	72,44
P 230	8	140	Zusammenstoß	GZ-RZ / RZ-RZ	120 < V ≤ 160	10	3,43E-08	3,89%	13,19
M 230	10	140	Zusammenstoß	GZ-RZ / RZ-RZ	120 < V ≤ 160	10	7,62E-08	3,26%	29,32
P 160 I	12	100	Zusammenstoß	GZ-RZ / RZ-RZ	80 < V ≤ 120	3	4,48E-08	4,94%	17,24
P 160 II	6	100	Zusammenstoß	GZ-RZ / RZ-RZ	80 < V ≤ 120	3	1,26E-08	10,92%	4,85
M 160	10	100	Zusammenstoß	GZ-RZ / RZ-RZ	80 < V ≤ 120	3	3,73E-08	18,52%	14,37
G 120	8	50	Zusammenstoß	GZ-GZ	40 < V ≤ 80	0,1	1,12E-09	17,06%	0,43
R 120	4	70	Zusammenstoß	GZ-RZ / RZ-RZ	40 < V ≤ 80	1	2,25E-09	26,33%	0,87
R 80	2	50	Frontal- zusammenstoß	GZ-RZ / RZ-RZ	80 < V ≤ 120	3	4,72E-09	10,07%	1,82
G 50	1	25	Frontal- zusammenstoß	GZ-GZ	40 < V ≤ 80	0,1	8,85E-11	1,55%	0,03

D_{AR}: Mittlere Betriebsdichte (Züge/Std. alle Richtungen) nach [95]

V_B: Mittlere Beförderungsgeschwindigkeit (km/h), eingeschätzt

S: Schadensausmaß (Opfer/Versagen)

BR_R: Betriebsrisiko pro Std. im Regelbetrieb am Beispiel eines Fdl-Steuerbereichs mit einer Gleislänge von 80 km

GL_A: Anteil der Gleislänge im Bereich der DB Netz AG nach [45, 95] eingeschätzt

RG_A: Angepasster Risikogrenzwert eines Kalenderjahrs nach Risiko und Anteil des Streckenstandards (Opfer/Jahr)

Das öffentliche Schienennetz hat in Deutschland nach dem Statistischen Bundesamt eine gesamte Gleislänge von ca. 67.400 km [93]. Bei der Anwendung der Bewertungssystematik werden aber lediglich die von Zügen planmäßig befahrenen Gleise bzw. die Hauptgleise berücksichtigt. Aufgrund der in den Daten des Statistischen Bundesamts fehlenden Angaben zur Länge des Hauptgleises wird dessen Länge im öffentlichen Schienennetz mittels des Hauptgleis-Anteils im Bereich der DB Netz AG eingeschätzt. Nach [45] haben die Hauptgleise im Bereich der DB Netz AG im Jahr 2017 eine gesamte Gleislänge von ca. 55.000 km. Das entspricht einen Anteil von ca. 91% der gesamten Gleislänge von ca. 60.500 km im Bereich der DB Netz AG. Dementsprechend wird die Gesamtlänge des Hauptgleises im öffentlichen Schienennetz in Deutschland anteilig auf ca. 61.300 km (= 67.400 km*91%) geschätzt. Unter

der Annahme einer äquivalenten Aufteilung des Betriebsrisikos über das ganze Netz lässt sich der Risikogrenzwert eines Fdl-Steuerbereichs pro Kalenderjahr (RG_{BJ}) als Produkt aus dem Risikogrenzwert des gesamten Netzes pro Kalenderjahr (RG_{NJ}) und dem Quotienten aus der Gleislänge eines Fdl-Bereichs (GL_B) und der gesamten Gleislänge im Netz (GL_N) anteilig bestimmen, wie die Formel (4) zeigt. Wird z. B. wie im Beispiel in Kapitel 4 ein Fdl-Steuerbereich mit einer Gleislänge von 80 km betrachtet, lässt sich durch die gegebene Formel ein Risikogrenzwert eines Fdl-Steuerbereichs pro Kalenderjahr von 1,87E-02 Opfern/Jahr (= 14,37 Opfer/Jahr * 80 km / 61.300 km) ableiten.

$$RG_{BJ} = RG_{NJ} * \frac{GL_B}{GL_N} \quad (4)$$

RG_{BJ} : Risikogrenzwert eines Fdl-Steuerbereichs pro Kalenderjahr (Opfer/Jahr)

RG_{NJ} : Risikogrenzwert des gesamten Netzes pro Kalenderjahr (Opfer/Jahr)

GL_B : Gleislänge eines betrachteten Fdl-Steuerbereichs (km)

GL_N : Gleislänge in dem gesamten Netz (km)

3.3.3 Mit der Risiko-Budgetierung zur proaktiven Steuerung des Betriebsrisikos

Zur Gestaltung eines Rückfallebenenkonzepts sowie zur proaktiven Steuerung des Betriebsrisikos wird in der vorliegenden Arbeit das Konzept der Risiko-Budgetierung aus dem Finanzwesen adaptiert. Im Bereich des sicherheitsrelevanten Systems ist die Anwendung einer solchen aktiven Risiko-Budgetierung zur Steuerung des Betriebsrisikos bisher unbekannt. Es gibt zwar das Konzept des Risikobudgets beim Risikomanagement, indem der Risikogrenzwert bzw. die Risikoakzeptanz eines sicherheitsrelevanten Systems als Risikobudget bezeichnet wird [96–99]. Eine Budgetierung von Risiken zur proaktiven Steuerung des Betriebsrisikos im Verlauf der Betriebsführung ist aber im Kontext des bekannten Risikobudgets nicht gegeben.

Das Konzept der Risiko-Budgetierung hat seinen Ursprung im Finanzwesen und ist eine verbreitete Methode zur aktiven Aufstellung und Steuerung eines Investitionsportfolios. Anstatt die Investitionssumme gleichmäßig auf die verschiedenen Finanzprodukte zu verteilen, wird die gesamte Investitionssumme eines Investitionsportfolios durch die Risiko-Budgetierung nach dem Risiko des jeweiligen Finanzproduktes anteilmäßig auf die verschiedenen Finanzprodukte verteilt und aktiv an die Marktentwicklung angepasst. Dadurch wird sichergestellt, dass im Zeitraum der Betrachtung das gesamte Investitionsrisiko der verschiedenen Finanzprodukte einen bestimmten Risikorahmen, auch bekannt als Tracking Error, welcher die Abweichung der Wertentwicklung des Investitionsportfolios einer Vergleichsbasis darstellt, nicht überschreitet [100–104].

Die Anwendung der Risiko-Budgetierung in der vorliegenden Arbeit zur Gestaltung eines Rückfallebenenkonzepts und zur proaktiven Steuerung des Betriebsrisikos hat zwar ihr Ursprung im Finanzwesen, unterscheidet sich aber in ihrer Vorgehensweise bei der Betrachtung des gesamten Risikos. Das Grundprinzip der Risiko-Budgetierung gibt vor, dass das gesamte

Risiko mehrerer Betrachtungsgegenstände einen bestimmten Risikogrenzwert im Zeitraum der Betrachtung nicht überschreiten sollte. Im Finanzwesen werden bei der Ermittlung des gesamten Risikos mehrere Betrachtungsgegenstände bzw. Finanzprodukte gleichzeitig berücksichtigt. Das aktuelle gesamte Risiko stellt ein relatives Risiko zu der Vergleichsbasis dar und umfasst lediglich die Risiken aller Finanzprodukte zum Zeitpunkt der Betrachtung. Die Risiken aller Finanzprodukte in den vergangenen Zeiten werden nicht als Teil des aktuellen gesamten Risikos berücksichtigt. Im Vergleich dazu besteht das aktuelle gesamte Betriebsrisiko in der vorliegenden Arbeit aus allen Betriebsrisiken des einzelnen vergangenen Zeitpunkts seit Beginn eines Betrachtungszeitraums. Das bedeutet, dass das gesamte Betriebsrisiko im Laufe der Zeit kumuliert wird.

Nach der Theorie der Risiko-Budgetierung lässt sich das Betriebsrisiko des Bahnbetriebs durch die Anwendung von unterschiedlichen Betriebskonzepten im Regelbetrieb sowie in Rückfallebenenkonzepten im Störungsbetrieb budgetieren, solange das kumulierte gesamte Betriebsrisiko im Bereich und Zeitraum der Betrachtung den ausgewählten Risikogrenzwert nicht überschreitet. Es ist aber zu diskutieren, inwieweit der ausgewählte Risikogrenzwert bei der Bewertung verbindlich ist. Dies hat die folgenden Gründe: Auch, wenn der Risikogrenzwert im Bereich und Zeitraum der Betrachtung überschritten wurde, heißt das nicht, dass unbedingt Unfälle passieren werden. Interpretiert werden kann nur, dass im Vergleich zu anderen Bereichen im Bereich und Zeitraum der Betrachtung ein höheres Betriebsrisiko bei der Überschreitung des Risikogrenzwerts erwartet wird. Der zweite Grund ist, dass der Risikogrenzwert eines einzelnen betrachteten Bereichs und Zeitraums, was in der Bewertungssystematik einen Fdl-Steuerbereich und ein Kalenderjahr umfasst, aus dem Risikogrenzwert des gesamten öffentlichen Schienennetzes pro Kalenderjahr nach Formel (4) anteilig bestimmt wird. Diese längenbezogene Aufteilung ermöglicht zwar eine äquivalente Aufteilung des Betriebsrisikos über das ganze Netz, heißt aber nicht, dass die Störungen während eines Betrachtungszeitraums in allen Fdl-Steuerbereichen in gleichem Maße passieren werden. In der Realität betreffen die Störungen während eines Kalenderjahrs nur einen Teil des Netzes und das außerdem in unterschiedlichem Maße. Das bedeutet, dass der gleichmäßig zugeteilte Risikogrenzwert bzw. die Risikoreserve eines Fdl-Steuerbereichs pro Kalenderjahr in einigen Fdl-Steuerbereichen nicht ausreichen wird, während es in vielen Fdl-Steuerbereichen einen Überschuss an Risikoreserve geben wird.

Nach dem Konzept der Risiko-Budgetierung ist die Nutzung der vorhandenen Risikoreserve aus den anderen Netzbereichen zulässig, solange der Risikogrenzwert des gesamten Netzes pro Kalenderjahr nicht überschritten wird. Um einerseits die Gestaltungsfreiheit eines Rückfallebenenkonzepts gewähren zu können und andererseits den Risikogrenzwert des gesamten Netzes pro Kalenderjahr einzuhalten, wird bei der Anwendung dieser Bewertungssystematik vorgeschlagen, während der Bewertung nur den Risikogrenzwert des gesamten Netzes pro Kalenderjahr als verbindlich anzusehen. Begründet wird dies damit, dass der Risikogrenzwert des gesamten Netzes aus der Unfallstatistik abgeleitet wurde. Im Gegensatz dazu kann der Risikogrenzwert eines einzelnen betrachteten Bereichs bzw. eines

Fdl-Steuerbereichs zwecks der Gestaltungsflexibilität im angemessenen Maße überschritten werden. Dieser Ansatz ermöglicht zwar eine größere Gestaltungsfreiheit eines Rückfallebenenkonzepts, birgt aber auch die Gefahr in sich, dass ein Rückfallebenenkonzept, welches ein übermäßig hohes stündliches Betriebsrisiko hat, aufgrund der hohen verfügbaren Risikoreserve am Ende des Betrachtungszeitraums bei einer Störung mit kurzer Dauer zugelassen wird. Konzeptionell ist ein solches Vorgehen nach dem Grundprinzip der Risiko-Budgetierung zwar erlaubt, in der Praxisumsetzung kann es aber zu einer kritischen gesellschaftlichen Debatte führen. Das liegt daran, dass die Fahrgäste der betroffenen Zugfahrten nach dem Risikomodell mit einer deutlich höheren Wahrscheinlichkeit zum Unfallopfer werden und / oder ein hohes Schadensausmaß bei einem Unfall haben werden.

Um das Rückfallebenenkonzept mit einem übermäßig hohen stündlichen Betriebsrisiko ausschließen zu können, muss sichergestellt werden, dass dessen stündliches Betriebsrisiko einen bestimmten stündlichen Risikogrenzwert nicht überschreitet. Nach dem Prinzip der Risiko-Budgetierung darf ein Rückfallebenenkonzept zeitlich länger angewendet werden, wenn das stündliche Betriebsrisiko dieses Rückfallebenenkonzepts kleiner ist. Umgekehrt darf ein Rückfallebenenkonzept nur selten angewendet werden, wenn dessen stündliches Betriebsrisiko höher ist. Dadurch kann das maximal zulässige stündliche Betriebsrisiko eines Rückfallebenenkonzepts durch die Festlegung einer durchschnittlichen zulässigen Anwendungsdauer des Rückfallebenenkonzepts in einem Fdl-Steuerbereich pro Kalenderjahr eingeschränkt werden. Die durchschnittliche zulässige Anwendungsdauer des Rückfallebenenkonzepts wird im Rahmen dieser Arbeit durch die durchschnittliche Stundenzahl des Störungsbetriebs in einem Fdl-Steuerbereich pro Kalenderjahr abgebildet.

Zur groben Einschätzung der Stundenzahl des Störungsbetriebs kann in Deutschland als öffentlich zugängliche Datenquelle im Bereich der DB Netz AG z. B. der jährlich veröffentlichte Infrastrukturzustands- und Entwicklungsbericht herangezogen werden. Im Bereich der DB Netz AG wird jede Störung nach der Priorität der Abarbeitung der Mängelbeseitigung vom Betrieb mit der Meldung eingestuft. Insgesamt werden 7 Prioritätsstufen vorgegeben, wobei die Störungen mit längeren betrieblichen Auswirkungen wesentlich den Prioritäten 1 bis 4 zugeordnet werden. Wie die Tabelle 10 zeigt, erfordern die Störungen der Prioritäten 1 und 2 eine sofortige Entstörung. Bei Priorität 1 (Unfall) ist außerdem eine sofortige Verständigung der Entstörbeauftragten und unverzügliches Aufsuchen der Unfallstelle erforderlich, während die Störung der Priorität 2 nach den definierten Eingreifzeiten je Objektgruppe entstört wird. Im Vergleich dazu sind die Störungen der Prioritäten 3 und 4 stapelbar. Bei Priorität 3 entscheidet die BZ und bei Priorität 4 der Fdl über den Termin der Entstörung. Die Stufe Priorität 5 wird nicht mehr verwendet. Eine Störung ohne betriebliche Auswirkungen wird als Priorität 6 eingestuft. Die letzte Stufe Priorität 7 umfasst die Einmalstörung, die in der Regel ohne Instandhaltungspersonal direkt durch den Fdl behoben werden kann [105].

Tabelle 10: Prioritäten von Störungen bei der DB Netz AG nach [105, 106]

Prioritäten	Art der Störung	Sofortige Handlung
Priorität 1	Unfall	Sofortige Verständigung der Entstörbeauftragten, unverzügliches Aufsuchen der Unfallstelle
Priorität 2	Entstörung sofort	Entsprechend der je Objektgruppe definierten Eingreifzeiten der Instandhaltung und während Inspektionen festgestellte Störungen mit ad-hoc-Maßnahmen
Priorität 3	Stapelbar BZ	BZ entscheidet über den Termin für die Beseitigung der Störung und deren mögliche betriebliche Auswirkungen.
Priorität 4	Stapelbar Fdl	Fdl entscheidet mit Fachdienst und Disponent über die terminliche Beseitigung der Störung und gibt den spätesten Entstörzeitpunkt vor
Priorität 5	(wird nicht mehr verwendet)	(bleibt leer)
Priorität 6	Fehler ohne betriebliche Auswirkung	k. A.
Priorität 7	Einmalstörung	Diese Störungen werden in der Regel ohne Instandhaltungspersonal durch den Fdl behoben.

Neben der Priorität der Störung wird auch die Zeitdauer, welche vom Auftreten der Störung bis zum Freigeben des gestörten Objekts nach der erfolgreichen Entstörung vergeht, ebenfalls dokumentiert. Diese Zeiten messen die unmittelbare Wirkung der aufgetretenen Störung auf den Bahnbetrieb und werden im Infrastrukturzustands- und Entwicklungsbericht (IZB) als Störbestehenszeiten bezeichnet. Wie die Tabelle 11 zeigt, beträgt die Summe der Störbestehenszeiten der Prioritäten 1 und 2 im Bereich der DB Netz AG im Zeitraum von 2010 bis 2018 im Durchschnitt 9.536.104 Min im Jahr. Mehr als die Hälfte (53,98%) der Störbestehenszeiten kann der Kategorie Leit- und Sicherungstechnik zugeordnet werden. Im Vergleich dazu haben die Störbestehenszeiten, deren Ursache auf die bauliche Infrastruktur (Gleise, Brücken und Tunnel) zurückzuführen sind, lediglich einen geringen Anteil von 4,28% in den gesamten Störbestehenszeiten.

Tabelle 11: Mittlere Störbestehenszeiten im Bereich der DB Netz AG im Zeitraum von 2010 bis 2018

Mittlere Störbestehenszeit Priorität 1 & 2 im Zeitraum 2010 bis 2018¹	In absoluten Zahlen (Min/Jahr)	Im Anteil (%)
Summe Störbestehenszeiten von Priorität 1 & 2	9.536.104	100,00%
dv. Leit- und Sicherungstechnik	5.146.270	53,98%
dv. Bahnübergänge	2.074.897	21,81%
dv. Weichen und Kreuzungen	1.688.932	17,66%
dv. Gleise	382.782	3,98%
dv. Selbstblocksignale	214.343	2,27%
dv. Brücken	12.707	0,13%
dv. Tunnel in Untertagebauweise	12.004	0,13%
dv. Tunnel in offener Bauweise	4.168	0,04%
1: Mittelwert aus dem Infrastrukturzustands und –entwicklungsbericht der DB Netz AG [45, 105, 107]		

Da in den öffentlich zugänglichen Berichten der DB Netz AG lediglich die Störbestehenszeiten der Prioritäten 1 und 2 veröffentlicht wurden, wird in der folgenden Beispielrechnung zur Einschätzung der Stundenzahl des Störungsbetriebs eines Kalenderjahrs die Annahme getroffen, dass die Störungen der Prioritäten 1 und 2 angesichts ihrer höheren Prioritäten auch größere betriebliche Auswirkungen haben werden. Infolgedessen wird davon ausgegangen, dass die Störbestehenszeiten der Prioritäten 1 und 2 für die Beispielrechnung in dieser Arbeit maßgeblich sind und dadurch der Stundenzahl des Störungsbetriebs in einem Kalenderjahr in der Größenordnung entsprechen sollten. Trotzdem werden in der vorliegenden Arbeit bei der Einschätzung der vsl. Stundenzahl von Störungen nicht alle Störbestehenszeiten der Prioritäten 1 und 2 mit 100% berücksichtigt. In der anschließenden Beispielberechnung werden in der eingeschätzten Stundenzahl von Störungen lediglich die Störungen mit den Ursachen Leit- und Sicherungstechnik, Weichen und Kreuzungen sowie Selbstblocksignale mit 100% berücksichtigt, während die Störbestehenszeiten der übrigen Ursachen Bahnübergänge, Gleise, Brücken und Tunnel mit nur 50% berücksichtigt werden.

Dies wird damit begründet, dass ein Unfall am Bahnübergang nur passieren kann, wenn sich externe Verkehrsteilnehmer und das Schienenfahrzeug zugleich auf dem Bahnübergang befinden. D. h.: Wenn sich kein externer Verkehrsteilnehmer auf dem Bahnübergang befindet, kann es auch keinen Schaden geben. Demzufolge besteht in den Zeiten ohne externe Verkehrsteilnehmer auf dem Bahnübergang auch kein Betriebsrisiko. Da ein Bahnübergang nicht stets von den externen Verkehrsteilnehmern benutzt wird, wird in der hier vorliegenden Beispielrechnung die Annahme getroffen, dass der Bahnübergang in 50% der Störbestehenszeiten bis zur Aufhebung der Störung von externen Teilnehmern belegt wurde und in 50% der Störbestehenszeiten nicht. Bei der Betrachtung von den Gleisen, Brücken und Tunneln wird berücksichtigt, dass die gestörten baulichen Infrastrukturen bis zur Aufhebung der Störung entweder befahrbar oder nicht befahrbar sind. Sind die baulichen Infrastrukturen während der Störungsdauer nicht befahrbar, dann besteht wegen des Betriebsausfalls im betroffenen Bereich bis zur Aufhebung der Störung kein Betriebsrisiko. Aus diesem Grund werden bei der Einschätzung der vsl. Stundenzahl von Störungen ebenfalls nur 50% der Störbestehenszeiten der baulichen Infrastrukturen aus dem IZB einberechnet.

Unter den oben genannten Annahmen lässt sich die vsl. Stundenzahl von Störungen im gesamten Netz pro Kalenderjahr mit 8.377.044 Min/Jahr oder 139.617 Std./Jahr neu berechnen. Da die Störungen auf jedem Kilometer im Netz auftreten können, wird die vsl. Stundenzahl von Störungen gleichmäßig nach der Netzlänge aufgeteilt. Dadurch lässt sich bei einer Hauptgleislänge von ca. 55.000 km im Bereich der DB Netz AG [45] mit einem Standardfehler von $\pm 0,0002$ Std./km-Jahr eine vsl. Stundenzahl von Störungen in Höhe von 2,53 Std./km-Jahr ableiten. Wird, wie im Beispiel in Kapitel 4, ein Fdl-Steuerbereich mit einer Gleislänge von 80 km betrachtet, ergibt sich in dem betrachteten Fdl-Steuerbereich eine durchschnittliche vsl. Stundenzahl von Störungen von ca. 205 Std./Jahr ($= 80 \text{ km} * 2,53 \text{ Std./km-Jahr}$) mit einem Standardfehler von $\pm 10,0$ Std./Jahr ($= 80 \text{ km} * \pm 0,0002 \text{ Std./km-Jahr}$). Bei einer Normalverteilung mit einem Vertrauensintervall von 95% ($205 \text{ Std./Jahr} \pm 2*10,0 \text{ Std./Jahr}$)

liegt die Untergrenze der vsl. Stundenzahl von Störungen in dem betrachteten Fdl-Steuerbereich dann bei ca. 185 Std./Jahr. Diese Untergrenze kann dann zur Einschränkung des Rückfallebenenkonzepts als die durchschnittliche zulässige Anwendungsdauer eines Rückfallebenenkonzepts in dem betrachteten Fdl-Steuerbereich angewandt werden. Das bedeutet, dass ein Rückfallebenenkonzept in diesem betrachteten Fdl-Steuerbereich erst zur Anwendung zugelassen wird, wenn dessen spezifische zulässige Anwendungsdauer pro Kalenderjahr gleich oder größer als 185 Std./Jahr ist. Des Weiteren kann zum Ausgleich der statischen Unsicherheit auch ein höherer Grenzwert anstatt der Untergrenze des 95% Vertrauensintervalls festgelegt werden. Die Entscheidung liegt dann bei dem Anwender.

Durch die Einhaltung der durchschnittlichen zulässigen Anwendungsdauer eines Rückfallebenenkonzepts lässt sich zwar vermeiden, dass ein Rückfallebenenkonzept mit einem übermäßig hohen stündlichen Betriebsrisiko bei der Risiko-Budgetierung zugelassen wird. Allerdings ist es nicht möglich, dadurch sicherzustellen, dass deswegen der Risikogrenzwert des gesamten Netzes pro Kalenderjahr nicht überschritten wird. Der Grund dafür ist, dass die aus den Störungsstatistiken ermittelte durchschnittliche zulässige Anwendungsdauer eines Rückfallebenenkonzepts ein Mittelwert ist, während die tatsächliche Stundenzahl der Störung von Jahr zu Jahr mal mehr und mal weniger im Bereich des statistischen Mittelwerts liegen kann. D. h.: Wird ein gleiches Rückfallebenenkonzept für alle Fdl-Steuerbereiche im gesamten Netz angewendet, dessen spezifische zulässige Anwendungsdauer in einem Kalenderjahr genau der statistischen Untergrenze der durchschnittlichen zulässigen Anwendungsdauer entspricht, muss im Laufe des Kalenderjahrs sichergestellt werden, dass die Summe der tatsächlichen Stundenzahl der Störung aus allen Fdl-Steuerbereichen die Untergrenze der vsl. Stundenzahl der Störung im gesamten Netz nicht überschreiten darf. Andernfalls kann der Risikogrenzwert des gesamten Netzes pro Kalenderjahr nicht eingehalten werden⁵.

Um den Risikogrenzwert des gesamten Netzes pro Kalenderjahr einhalten zu können, wird in dieser Arbeit eine proaktive Steuerung der Risikoentwicklung als Lösungsansatz vorgeschlagen. Durch die proaktive Steuerung soll sichergestellt werden, dass die kumulierte Summe des Betriebsrisikos im gesamten Netz vom Beginn des Kalenderjahrs bis zum Zeitpunkt der Betrachtung einen Richtwert nicht überschreitet. Unter der Annahme einer konstanten Anstiegsrate des Betriebsrisikos lässt sich, wie die Formel (5) zeigt, der entsprechende Richtwert zu jedem Zeitpunkt der Betrachtung als Produkt aus dem Risikogrenzwert des gesamten Netzes pro Kalenderjahr (RG_{NJ}) und dem Quotient aus der vergangenen Betriebsdauer seit Beginn des Kalenderjahrs (BD_{Ti}) und der voraussichtlichen gesamten Betriebsdauer eines Kalenderjahrs (BD_J) bestimmen. Dieser ermittelte Richtwert wird im Folgenden als temporärer Risikogrenzwert (TRG_{Ni}) bezeichnet. Der temporäre Risikogrenzwert gilt nur als Orientierungswert zur proaktiven Steuerung der Risikoentwicklung, ist aber nicht

⁵ Bei diesem Beispiel wird vereinfacht angenommen, dass die einzelnen Störungen in einem Kalenderjahr in allen Fdl-Steuerbereichen immer gleich sind (z. B. die Dauer und das Ausmaß) und immer mit dem gleichen Rückfallebenenkonzept behandelt werden.

als verbindlich anzusehen. Dennoch darf der temporäre Risikogrenzwert den Risikogrenzwert des gesamten Netzes pro Kalenderjahr zu keinem Zeitpunkt überschreiten.

$$TRG_{Nt} = RG_{NJ} * \frac{BD_{Zt}}{BD_J} \quad (5)$$

TRG_{Nt} : Temporärer Risikogrenzwert des gesamten Netzes zum Zeitpunkt t (Opfer/Jahr)

RG_{NJ} : Risikogrenzwert des gesamten Netzes pro Kalenderjahr (Opfer/Jahr)

BD_{Zt} : Die vergangene Betriebsdauer von Beginn des Kalenderjahrs bis zum Zeitpunkt t (Std.)

BD_J : Die voraussichtliche Betriebsdauer eines Kalenderjahrs (Std.)

Die Annahme einer konstanten Anstiegsrate des Betriebsrisikos im Laufe eines Kalenderjahrs ist begründet, da die Entwicklung des Betriebsrisikos hier auf der Ebene des gesamten Netzes makroskopisch betrachtet wird. Die Störungen in einem Fdl-Steuerbereich treten im Laufe eines Kalenderjahrs in der Regel nur zu beliebigen Zeitpunkten auf und haben eine unbestimmte Störungsdauer. Eine Annahme eines konstanten Anstiegs des Betriebsrisikos kann bei der Betrachtung eines einzigen Fdl-Steuerbereichs nicht erfolgen, da die Störungen nur in einigen Zeitabschnitten eines Kalenderjahrs in dem Bereich auftreten und das damit verbundene Betriebsrisiko in der Regel höher als in den übrigen Zeitabschnitten im normalen Betrieb ist. Im Vergleich dazu kann die Annahme eines konstanten Anstiegs des Betriebsrisikos unter einer makroskopischen Betrachtung in Bezug auf das gesamte Netz erfolgen. Wenn die Grundgesamtheit bzw. die Anzahl der Fdl-Steuerbereiche groß ist, können die Störungen zu jedem beliebigen Zeitpunkt sowie an jeder beliebigen Stelle auftreten. Damit lässt sich annehmen, dass sich zu jedem Zeitpunkt in einem Kalenderjahr immer ein Teil des gesamten Netzes im Störungsbetrieb befinden wird, dessen Anteil am gesamten Netz als konstant anzusehen ist. Das bedeutet, dass sich der Zeitpunkt des Auftretens von Störungen aus Sicht des gesamten Netzes auf der Zeitachse eines Kalenderjahrs gleichmäßig aufteilen wird und dadurch ein konstanter Anstieg des Betriebsrisikos erfolgen kann.

Zur proaktiven Steuerung der Risikoentwicklung werden folgende Prinzipien verfolgt: Neigt die Entwicklung des Betriebsrisikos im gesamten Netz im Laufe des Kalenderjahrs dazu, den temporären Risikogrenzwert zu überschreiten, kann die Entwicklung des Betriebsrisikos durch die Erhöhung der durchschnittlichen zulässigen Anwendungsdauer eines Rückfallebenenkonzepts abgebremst werden. Fällt die Entwicklung des Betriebsrisikos im gesamten Netz deutlich unter den temporären Risikogrenzwert, lassen sich die Lösungsräume des Rückfallebenenkonzepts durch die Absenkung der durchschnittlichen zulässigen Anwendungsdauer eines Rückfallebenenkonzepts erweitern, jedoch maximal bis zur Untergrenze eines ausgewählten Vertrauensintervalls⁶. Dementsprechend muss bei der Umsetzung dieser Prinzipien festgelegt werden, zu welchem Zeitpunkt eine Anpassung der

⁶ Das maximale stündliche Betriebsrisiko eines Rückfallebenenkonzepts wird durch die Erhöhung der durchschnittlichen zulässigen Anwendungsdauer vom Rückfallebenenkonzept reduziert. Umgekehrt wird das maximale stündliche Betriebsrisiko eines Rückfallebenenkonzepts durch die Absenkung der durchschnittlichen zulässigen Anwendungsdauer vom Rückfallebenenkonzept erhöht.

durchschnittlichen zulässigen Anwendungsdauer eines Rückfallebenenkonzepts erforderlich ist. Als Kriterium zum Zeitpunkt der Anpassung wird im Rahmen dieser Arbeit eine Verhältnisgrenze⁷ auf ein temporäres Risikoverhältnis (TRV_{Nt}) gesetzt, welches als Verhältnis zwischen der kumulierten Summe des Betriebsrisikos im gesamten Netz vom Beginn des Kalenderjahrs bis zum Zeitpunkt t (KBR_{Nt}) und dem temporären Risikogrenzwert des gesamten Netzes zum Zeitpunkt t (TRG_{Nt}) in Prozent dargestellt wird, wie die Formel (6) zeigt.

$$TRV_{Nt} = \frac{KBR_{Nt}}{TRG_{Nt}} * 100 \quad (6)$$

TRV_{Nt} : Temporäres Risikoverhältnis des gesamten Netzes zum Zeitpunkt t (%)

KBR_{Nt} : Summe des kumulierten Betriebsrisikos in dem gesamten Netz vom Beginn des Kalenderjahrs bis zum Zeitpunkt t (Opfer/Jahr)

TRG_{Nt} : Temporärer Risikogrenzwert des gesamten Netzes zum Zeitpunkt t (Opfer/Jahr)

Die Kontrolle über das aktuelle temporäre Risikoverhältnis kann z. B. im wöchentlichen Rhythmus stattfinden. Da sich die Kontrolle der Entwicklung des Betriebsrisikos an dieser Stelle auf der Ebene des gesamten Netzes befindet, kann angenommen werden, dass dieser Zeitabstand für den gegebenen Zweck angemessen ist. Dennoch sollte im Fall einer netzweiten oder großräumigen Störung vor der Umsetzung eines Rückfallebenenkonzepts eine zusätzliche Kontrolle durchgeführt werden, um sicherzustellen, dass die prognostizierte Entwicklung des Betriebsrisikos den temporären Risikogrenzwert am nächsten Kontrollzeitpunkt nicht abrupt oder übermäßig überschreiten wird. Sollte bei der Kontrolle festgestellt werden, dass das aktuelle oder prognostizierte temporäre Risikoverhältnis zwischen beiden Parametern eine ausgewählte Verhältnisgrenze ($GTRV_{Nt}$) von z. B. 70% überschritten hat oder überschreiten wird, dann muss eine Erhöhung der durchschnittlichen zulässigen Anwendungsdauer eines Rückfallebenenkonzepts erfolgen. Das Maß der Anpassung ist dann gemäß dem Verhältnis des voraussichtlichen Anstiegs des kumulierten Betriebsrisikos im gesamten Netz, mit Beginn von dem aktuellen Zeitpunkt t bis zum nächsten Zeitpunkt $t + \Delta t$, mit und ohne der Anpassung zu bestimmen. Wie die Formel (7) zeigt, ergibt sich der vsl. Anstieg des kumulierten Betriebsrisikos mit der Anpassung aus der Differenz zwischen dem kumulierten Betriebsrisiko mit der Anpassung am Zeitpunkt $t + \Delta t$ ($KBR_{NMt+\Delta t}$) und dem kumulierten Betriebsrisiko zum aktuellen Zeitpunkt t (KBR_{Nt}). In ähnlicher Weise wird der vsl. Anstieg des kumulierten Betriebsrisikos ohne die Anpassung aus der Differenz zwischen dem kumulierten Betriebsrisiko ohne die Anpassung am Zeitpunkt $t + \Delta t$ ($KBR_{NOt+\Delta t}$) und dem kumulierten Betriebsrisiko zum aktuellen Zeitpunkt t (KBR_{Nt}) ausgerechnet. Das Verhältnis des voraussichtlichen Anstiegs (VA_N) wird in Prozent dargestellt.

⁷ In Prozentsatz

$$VA_N = \frac{KBR_{NM_{t+\Delta t}} - KBR_{N_t}}{KBR_{NO_{t+\Delta t}} - KBR_{N_t}} * 100 \quad (7)$$

- VA_N : Verhältnis des vsl. Anstiegs des kumulierten Betriebsrisikos im gesamten Netz (%)
 KBR_{N_t} : Aktuelle Summe des kumulierten Betriebsrisikos in dem gesamten Netz vom Beginn des Kalenderjahrs bis zum Zeitpunkt t (Opfer/Jahr)
 $KBR_{NM_{t+\Delta t}}$: Vsl. Summe des kumulierten Betriebsrisikos in dem gesamten Netz vom Beginn des Kalenderjahrs bis zum Zeitpunkt t+Δt mit der Anpassung ab Zeitpunkt t (Opfer/Jahr)
 $KBR_{NO_{t+\Delta t}}$: Vsl. Summe des kumulierten Betriebsrisikos in dem gesamten Netz vom Beginn des Kalenderjahrs bis zum Zeitpunkt t+Δt ohne die Anpassung (Opfer/Jahr)

Das Ergebnis der Rechnung ist dann wie folgt zu interpretieren und anzuwenden: Wird ein Verhältnis des vsl. Anstiegs von z. B. 50% bestimmt, dann bedeutet das, dass der vsl. Anstieg des kumulierten Betriebsrisikos ab dem aktuellen Zeitpunkt t mit der Anpassung im Vergleich zu dem Ergebnis ohne Anpassung bis zum Zeitpunkt t+Δt um 50% reduziert werden kann. Das heißt auch, dass das stündliche Betriebsrisiko des Rückfallebenenkonzepts unter der gleichen Anwendungsdauer um vsl. 50% reduziert werden muss. Hat sich das stündliche Betriebsrisiko eines Rückfallebenenkonzepts um die Hälfte verringert, dann verdoppelt sich zugleich die spezifische zulässige Anwendungsdauer eines Rückfallebenenkonzepts, da der Risikogrenzwert des gesamten Netzes pro Kalenderjahr konstant ist. D. h., dass im Fall einer Verdoppelung der durchschnittlichen zulässigen Anwendungsdauer eines Rückfallebenenkonzepts das maximale stündliche Betriebsrisiko eines Rückfallebenenkonzepts um vsl. 50% reduziert wird. Letztendlich wird das Verhältnis des vsl. Anstiegs des kumulierten Betriebsrisikos zwischen dem aktuellen Zeitpunkt t und dem nächsten Zeitpunkt t+Δt unter der gleichen prognostizierten Störungsdauer durch die Verdoppelung der durchschnittlichen zulässigen Anwendungsdauer um vsl. 50% reduziert. Das gleiche Prinzip gilt umgekehrt auch für die Reduzierung der durchschnittlichen zulässigen Anwendungsdauer eines Rückfallebenenkonzepts. Wird z. B. bei der Kontrolle festgestellt, dass sich die Entwicklung des Betriebsrisikos verlangsamt hat und dessen Verhältnis zum temporären Risikogrenzwert stetig in Richtung der Verhältnisgrenze sinkt, dann kann die durchschnittliche zulässige Anwendungsdauer eines Rückfallebenenkonzepts dementsprechend reduziert werden, maximal jedoch bis zur Untergrenze der statistisch ermittelten durchschnittlichen zulässigen Anwendungsdauer innerhalb des ausgewählten Vertrauensintervalls.

Zusammengefasst: Die Flexibilität der Risiko-Budgetierung bei der Gestaltung eines Rückfallebenenkonzepts wird im Konzept dieser Arbeit durch insgesamt drei Maßnahmen eingeschränkt, wie in Abbildung 15 dargestellt wird. Erstens: Der Risikogrenzwert des gesamten Netzes pro Kalenderjahr ist verbindlich und muss in der Regel eingehalten werden. Zweitens: Die spezifische zulässige Anwendungsdauer eines Rückfallebenenkonzepts in einem Fdl-Steuerbereich pro Kalenderjahr darf die durchschnittliche zulässige Anwendungsdauer eines Rückfallebenenkonzepts in der Regel nicht unterschreiten, damit kein Rückfallebenenkonzept mit einem übermäßig hohen stündlichen Betriebsrisiko zugelassen wird. Drittens: Die Entwicklung des Betriebsrisikos im gesamten Netz wird durch den

regelmäßigen Vergleich mit dem temporären Risikogrenzwert und der Anpassung der durchschnittlichen zulässigen Anwendungsdauer eines Rückfallebenenkonzepts proaktiv gesteuert. Dadurch wird ein abrupter Anstieg des Betriebsrisikos aufgrund der großen und / oder lange andauernden Störungen vermieden. Ebenfalls kann eine ausreichende Risikoreserve für die Gestaltungsfreiheit des Rückfallebenenkonzepts zu jedem Zeitpunkt gewährleistet werden. Im Endeffekt sollen all diese Maßnahmen dazu führen, dass die Sicherheit des Bahnbetriebs trotz der erweiterten Gestaltungsfreiheit eines Rückfallebenenkonzepts durch die Umsetzung der Risiko-Budgetierung weiterhin sichergestellt werden kann.

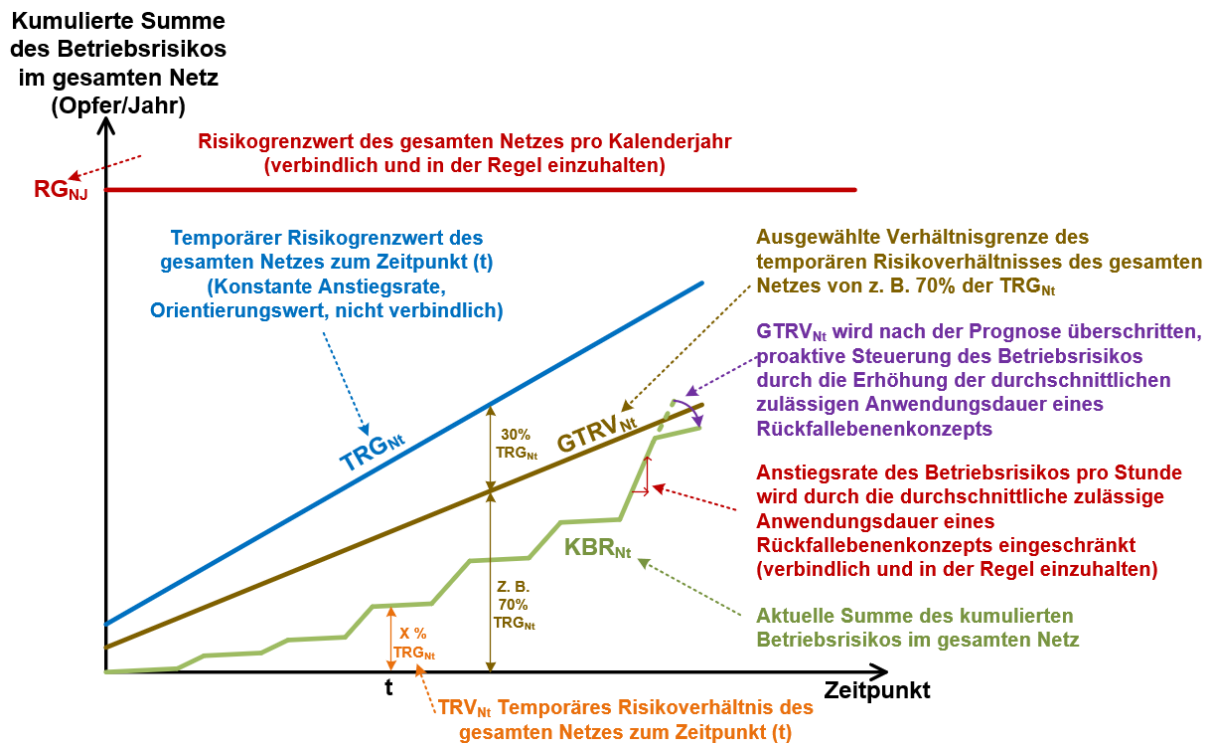


Abbildung 15: Maßnahmen zur Einschränkung der Flexibilität der Risiko-Budgetierung

3.4 Die risikoorientierte Bewertungssystematik

3.4.1 Das Risikomodell und die Übersicht der Systematik

Das Risikomodell dieser Bewertungssystematik betrachtet ein Eisenbahnsystem, welches den technischen und menschlichen Akteur umfasst und aus verschiedenen generischen Funktionen auf einer hohen Systemebene besteht. Die generischen Funktionen werden in der Bewertungssystematik anhand eines Funktionsmodells abgebildet (siehe Kapitel 3.4.2.2 für Detail). Da die Betrachtung der generischen Funktionen auf einer hohen Systemebene erfolgt, wird im Rahmen der Bewertung angenommen, dass ein Funktionsversagen im System der Betrachtung zugleich die Betriebsgefahr auf der Ebene des Bahnsystems zur Folge haben wird. Betriebliche Zustände und Umgebungsereignisse, die das Betriebsrisiko beeinflussen können, einschließlich der Auslastung der Menschen, der Bedrohungslage und des IT-Schutzniveaus des Systems, werden in dem Risikomodell im Rahmen des Betriebs- und Umgebungskontexts sowie der externen Barriere berücksichtigt, wie die Abbildung 16 darstellt. Nach EN 50126-2 enthält die externe Barriere jene betrieblichen Merkmale, die das Schadensausmaß eines potenziellen Unfalls reduzieren können [22]. In dem vorliegenden Risikomodell werden folgende betriebliche Merkmale als externe Barrieren bei der Ermittlung des Betriebsrisikos berücksichtigt: die Betriebsweise (Ein- oder Zweirichtungsbetrieb), die Betriebsdichte, die Betriebsgeschwindigkeit, und die Verkehrsart (Güterverkehr, Reiseverkehr oder Mischverkehr).

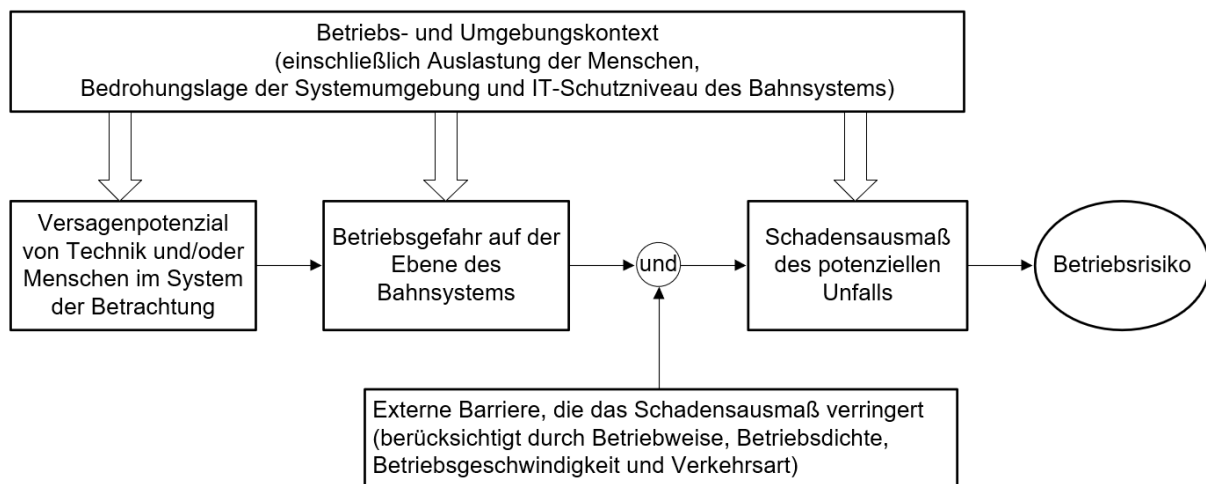


Abbildung 16: Risikomodell der vorliegenden Bewertungssystematik nach [22]

Nach dem vorliegenden Risikomodell lässt sich das Betriebsrisiko ($BR_{Bn,i}$) in einem betrachteten (Teil-)Bereich n im Zeitabschnitt i unter dem vorgegebenen Betriebs- und Umgebungskontext anhand der Variablen vsl. Anzahl der Versagen ($VS_{Bn,i}$), Verstärkungsfaktor aus dem IT-Manipulationspotenzial ($F_{ITn,i}$), Reduktionsfaktor aus der Betriebsdichte ($F_{Rn,i}$) und Schadensausmaß des Unfalls ($S_{Mn,i}$) formulieren, wie die Formel (8)

zeigt. Da die Variablen in der Formel (8) das Betriebsrisiko multiplikativ beeinflussen, ist die Annahme notwendig, dass die oben genannten Variablen voneinander unabhängig sind.

$$BR_{B_{n,i}} = VS_{B_{n,i}} * F_{IT_{n,i}} * F_{R_{n,i}} * S_{M_{n,i}} \quad (8)$$

- $BR_{B_{n,i}}$: Betriebsrisiko im (Teil-)Bereich n im Zeitabschnitt i unter dem vorgegebenen Betriebs- und Umgebungskontext (Opfer/Zeitabschnitt i)
 $VS_{B_{n,i}}$: Vsl. Anzahl der Versagen im (Teil-)Bereich n im Zeitabschnitt i (Versagen/Zeitabschnitt i)
 $F_{IT_{n,i}}$: Verstärkungsfaktor aus IT-Manipulationspotenzial im (Teil-)Bereich n im Zeitabschnitt i
 $F_{R_{n,i}}$: Reduktionsfaktor aus der Betriebsdichte im (Teil-)Bereich n im Zeitabschnitt i
 $S_{M_{n,i}}$: Schadensausmaß des Unfalls im (Teil-)Bereich n im Zeitabschnitt i (Opfer/Versagen)

Im Vergleich mit dem Risikomodell beschreibt die Variable VS_{Bi} das Versagenspotenzial der Technik und der Menschen im Bahnbetrieb unter dem Einfluss des betrachteten Betriebskontexts im Risikomodell. Die ausführliche Behandlung und Anwendung dieser Variable ist in Kapitel 3.4.2.1 bis Kapitel 3.4.2.4. zu finden. Der Verstärkungsfaktor F_{ITi} , dessen Details in Kapitel 3.4.2.5 behandelt werden, berücksichtigt die Auswirkung der Änderung im System und dessen Umgebung im Risikomodell auf das Betriebsrisiko mit dem Fokus auf den IT-Angriff. Zuletzt werden das Schadensausmaß und dessen zugehörige externe Barriere durch die Variable F_{Ri} und S_{Mi} im Risikomodell abgebildet, die dann in Kapitel 3.4.2.6 sowie Kapitel 3.4.2.7 behandelt werden. Wie die Abbildung 17 zeigt, besteht die risikoorientierte Bewertungssystematik aus sieben Strukturteilen.

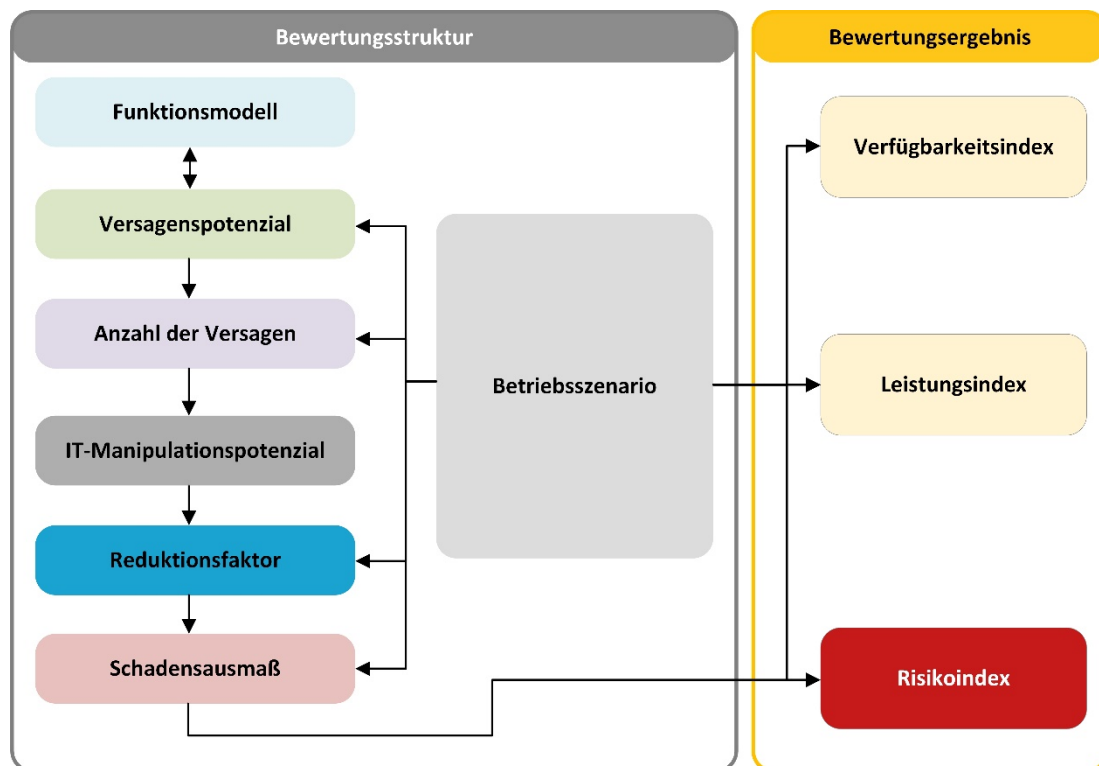


Abbildung 17: Strukturübersicht der risikoorientierten Bewertungssystematik

Dazu gehören⁸:

- das Betriebsszenario (Kapitel 3.4.2.1),
- das Funktionsmodell (Kapitel 3.4.2.2),
- das Versagenspotenzial (Kapitel 3.4.2.3),
- die Anzahl der Versagen (Kapitel 3.4.2.4),
- das IT-Manipulationspotenzial (Kapitel 3.4.2.5),
- der Reduktionsfaktor (Kapitel 3.4.2.6) und
- das Schadensausmaß (Kapitel 3.4.2.7).

Der Strukturteil Betriebsszenario enthält die Betriebsvariablen des aktuellen Betriebsszenarios. Das sind z. B. die Betriebsdichte, die Beförderungsgeschwindigkeit, die Größe des Steuerbereichs, die Größe des Störungsbereichs und die vsl. Dauer der Störung. Die Betriebsvariablen dienen als grundlegende Eingangsgrößen zur Bestimmung der Qualität von Rückfallebenenkonzepten und werden auch von anderen Strukturteilen benötigt. So wird z. B. die Betriebsdichte zur Anpassung der Versagenswahrscheinlichkeit von Menschen sowie zur Ableitung vom Reduktionsfaktor als Basis angewendet. Auch das Leistungsniveau und die technische Verfügbarkeit des betrachteten Szenarios lassen sich direkt aus den Betriebsvariablen ableiten.

Um das Risiko des Bahnbetriebs ermitteln zu können, wird die Abwicklung der Betriebsführung in einem entsprechenden Detail in der Bewertung berücksichtigt bzw. abgebildet. Durch den Strukturteil Funktionsmodell werden die Betriebsfunktionen, welche für die Realisierung einer sicheren Durchführung der Zugfahrt benötigt werden, generisch abgebildet. Es wird die Annahme getroffen, dass alle generischen Betriebsfunktionen in dem Funktionsmodell unabhängig voneinander sind. Das bedeutet, dass das Versagen einer einzelnen Betriebsfunktion des Funktionsmodells die Zugfahrt gleich in einen gefährlichen Betriebszustand führen kann. Für jede Betriebsfunktion in dem Funktionsmodell wird ein maßgeblicher Akteur identifiziert. Der Akteur ist entweder ein Mensch oder ein technisches System.

Im Strukturteil Versagenspotenzial wird das Versagenspotenzial des Rückfallebenenkonzepts basierend auf dem generischen Funktionsmodell abgeleitet. Da jede Betriebsfunktion voneinander unabhängig ist, können zur Ermittlung des Versagenspotenzials eines Funktionsmodells die Versagensraten der einzelnen Betriebsfunktionen direkt miteinander addiert werden. Das ist aber nur bei einem Regelbetrieb mit technischem System der Fall. Wird während des Störungsbetriebs mindestens eine der generischen Betriebsfunktionen vom Menschen als maßgeblicher Akteur übernommen, dann ist eine Addition wegen der verschiedenen Einheiten der technischen Versagensrate (Versagen/Betriebsstunde) und der menschlichen Versagenswahrscheinlichkeit (einheitslos) nur durch eine Umrechnung möglich.

⁸ Dieser Abschnitt beruht zum Teil auf der autoreigenen Veröffentlichung in [138]

Das Versagenspotenzial eines Funktionsmodells wird daher in diesem Strukturteil je nach dem maßgeblichen Akteur der Betriebsfunktion (technisches System oder Mensch) getrennt behandelt. Anders als die technische Versagensrate, für welche keine Anpassung im laufenden Betrieb vorgesehen wird, wird die Versagenswahrscheinlichkeit des Menschen nach der Gegebenheit des aktuellen Betriebsszenarios auslastungsbedingt angepasst. Die Versagenswahrscheinlichkeit des Fdl wird bei der Bewertung hinsichtlich dessen Handlungsdauer, Handlungsumfang sowie Handlungsintensität szenarioabhängig ermittelt. Im Vergleich dazu wird die Versagenswahrscheinlichkeit des Tf vereinfacht durch die Änderung von dessen Tätigkeiten zwischen dem Regel- und Störungsbetrieb bestimmt.

Der nächste Strukturteil Anzahl der Versagen liefert ein Zwischenergebnis der Bewertung. Mit der Anwendung einer Umrechnungsmethode, die im Rahmen dieser Systematik entwickelt wurde, wird eine Zusammenführung des Versagenspotenzials von Technik und Mensch ermöglicht. Das Versagenspotenzial eines Funktionsmodells im vorliegenden Betriebsszenario wird als eine einzige Ausgangsgröße zusammengefasst. Somit lässt es sich anschließend direkt bei der Ermittlung des Betriebsrisikos einsetzen

Angesichts der IT-Security-Bedrohung wird auch berücksichtigt, dass durch die dynamische Bedrohungslage sowohl die Versagensrate des technischen Systems als auch die Versagenswahrscheinlichkeit des Menschen zusätzlich beeinflusst werden können. Durch den Strukturteil IT-Manipulationspotenzial wird das aktuelle Manipulationspotenzial des Bahnbetriebs anhand des aktuellen IT-Schutzniveaus des Systems und der aktuellen IT-Bedrohungslage der Systemumgebung pauschal eingeschätzt. Das Ergebnis fließt dann als Verstärkungsfaktor in die Anzahl der Versagen mit ein.

Durch den Strukturteil Reduktionsfaktor wird berücksichtigt, dass das Eintreten eines Versagens nicht unbedingt einen Unfall zur Folge haben muss. Dies betrifft insbesondere die Unfallart Zusammenstoß, bei der gleichzeitig zwei Eisenbahnfahrzeuge involviert sein müssen. Falls sich jedoch nach dem Eintritt eines Versagens nur ein Eisenbahnfahrzeug im potenziellen Bereich der Kollision befindet, wird es auch keinen Zusammenstoß geben können. Der Reduktionsfaktor wird jedoch bei den anderen Unfallarten wie Entgleisung, Aufprall und Zusammenprall nicht angewendet, da die Beteiligung eines zweiten Fahrzeugs bei diesen Unfallarten nicht zwingend erforderlich ist.

Im letzten Strukturteil Schadensausmaß wird das Ausmaß eines Versagens eingeschätzt, falls es tatsächlich zum Unfall kommen sollte. Da in einem Funktionsmodell theoretisch mehrere Betriebsfunktionen gleichzeitig versagen können, wird hier bei der Einschätzung des Schadensausmaßes nur ein maßgebliches Versagen von einer bestimmten Betriebsfunktion berücksichtigt. Die Größe des Schadensausmaßes wird hier mit der Anzahl Opfer pro Versagen beschrieben. In Kombination mit dem Ergebnis aus dem Strukturteil Anzahl der Versagen lässt sich das Betriebsrisiko eines Rückfallebenenkonzepts als Anzahl Opfer pro Betrachtungszeitraum ermitteln.

Angelehnt an die semi-quantitative Risikobeurteilungsmethode, in der die zu bemessenen numerischen Werte in ein bestimmtes Intervall eingeteilt sind und über die Zuordnung zu den qualitativen Skalen verknüpft werden [86, 87], werden in der vorliegenden Arbeit zur Ermittlung der Variablenwerte die zu bemessenen numerischen Werte in ein ausgewähltes logarithmisches Intervall eingeteilt, die aber über die Zuordnung zu den verhältnisskalierten Ergebniswerten verknüpft werden. Die Bandbreite des Intervalls sollte nach [86] in der Regel nicht größer als 10 sein, was der Bandbreite des Safety-Integrity-Level (SIL) entspricht. Die gängigen semi-quantitativen Risikoanalyseverfahren arbeiten üblicherweise mit einer Bandbreite von ca. 3 bis 10, indem eine mittlere Ungenauigkeit um einen Faktor von ca. $\sqrt{3}$ bis $\sqrt{10}$ fachlich akzeptiert wird [86]. Die Bandbreite der gängigen Verfahren von ca. 3 führt bei der Beschreibung der Variablenwerte und des Ergebnisses im Rahmen dieser Arbeit aber zu einer undetaillierten Einteilung. Daher wird für die vorliegende Arbeit, außer für die Variable Schadensausmaß, als logarithmisches Intervall eine Bandbreite⁹ von ca. $\sqrt{3}$ gewählt.

Bei der Variable Schadensausmaß des Unfalls (S_{Mi}) wird ausnahmsweise ein Intervall von ca. 3 gewählt, da die Einflussfaktoren zur Ermittlung des Schadensausmaßes im Rahmen dieser Arbeit aus der deutschen Normung VDE V 0831-103 übernommen wurden und die Klassifizierung der Einflussfaktoren und deren Kombination in der Normung auf das Intervall von ca. 3 kalibriert sind. Eine Anwendung des Intervalls von ca. $\sqrt{3}$ würde eine neue Klassifizierung der Einflussfaktoren und deren Zuordnung zum Schadensausmaß erfordern, die angesichts des Schwerpunkts der Arbeit sowie des mit dieser Arbeit verbundenen Arbeitsaufwands nicht behandelt werden kann. Die Ableitung des Betriebsrisikos bleibt trotz der Differenz der Bandbreite weiterhin systematisch, da das Intervall von ca. 3 eine Potenz von ca. $\sqrt{3}$ ist.

Da die Differenzierung des Betriebsrisikos im Bereich der Betrachtung aus Sicht des Bereichszustands erfolgt, kann sich ein Steuerbereich des Fdl zugleich im Regel- und Störungsbetrieb befinden. Dadurch lässt sich das gesamte Betriebsrisiko in einem Fdl-Steuerbereich n im Zeitabschnitt i ($BR_{Bn,i}$) als Summe von dessen Betriebsrisiko im Teilbereich mit Störungsbetrieb ($BR_{BSn,i}$) und dessen Betriebsrisiko im Teilbereich mit Regelbetrieb ($BR_{BRn,i}$) ausrechnen, wie die Formel (9) zeigt.

$$BR_{Bn,i} = BR_{BSn,i} + BR_{BRn,i} \quad (9)$$

$BR_{Bn,i}$: Betriebsrisiko im betrachteten Fdl-Steuerbereich n im Zeitabschnitt i

$BR_{BSn,i}$: Betriebsrisiko im Teilbereich mit Störungsbetrieb im betrachteten Fdl-Steuerbereich n im Zeitabschnitt i

$BR_{BRn,i}$: Betriebsrisiko im Teilbereich mit Regelbetrieb im betrachteten Fdl-Steuerbereich n im Zeitabschnitt i

⁹ Die logarithmische Basis in dieser Bewertungssystematik beträgt genau ($\sqrt{3},16$). Diese Basis wird im weiteren Text mit „ca. $\sqrt{3}$ “ und in den Tabellen mit „ $\sqrt{3}$ “ vereinfacht dargestellt.

Im Rahmen dieser Arbeit wird die Länge des Zeitabschnitts für die einzelne Bewertung mit 1 Std. ausgewählt. Die Parameter der Systematik, die im anschließenden Kapitel 3.4.2 behandelt werden, wurden dem ausgewählten Zeitabschnitt entsprechend kalibriert. Dadurch umfasst das Ergebnis der einzelnen Bewertungen nach Formel (9) lediglich das Betriebsrisiko in einer betrachteten Stunde im einem bestimmten Fdl-Steuerbereich. Die Entwicklung des Betriebsrisikos eines bestimmten Fdl-Steuerbereichs in einem Kalenderjahr lässt sich dann von Beginn des Kalenderjahrs bis zu einem bestimmten Zeitpunkt t kumulativ erfassen, wie die Formel (10) darstellt.

$$KBR_{B_{n,t}} = \sum_{i=1}^p BR_{B_{n,i}} \quad (10)$$

- $KBR_{B_{n,t}}$: Kumuliertes Betriebsrisiko im betrachteten Fdl-Steuerbereich n von Beginn des Kalenderjahrs bis zum Zeitpunkt t (Opfer/Jahr)
- $BR_{B_{n,i}}$: Das Betriebsrisiko im betrachteten Fdl-Steuerbereich n in der Stunde i ($i = 1, \dots, p$) (Opfer/Jahr)
- i : Die fortlaufende Stundenzahl von Beginn des Kalenderjahrs bis zum aktuellen Zeitpunkt t
- p : Die letzte Stunde der Betrachtung vor dem aktuellen Zeitpunkt t , die der Anzahl der Stunden von Beginn des Kalenderjahrs bis zum aktuellen Zeitpunkt t entspricht

Um jedoch die Entwicklung des Betriebsrisikos in einem Kalenderjahr auf der Ebene des gesamten Netzes proaktiv steuern zu können, muss auch der aktuelle Stand des Betriebsrisikos im gesamten Netz nach dem Konzept Risiko-Budgetierung in Kapitel 3.3.3 bekannt sein. Dementsprechend muss das Betriebsrisiko jeder vergangenen Stunde aus jedem Fdl-Steuerbereich im Netz erfasst werden. Durch die Erweiterung der Formel (10) von einem Fdl-Steuerbereich auf alle Fdl-Steuerbereiche des gesamten Netzes lässt sich das kumulierte Betriebsrisiko im gesamten Netz von Beginn des Kalenderjahrs bis zum Zeitpunkt t anhand der Formel (11) sukzessiv ermitteln.

$$KBR_{N_t} = \sum_{n=1}^q \sum_{i=1}^p BR_{B_{n,i}} \quad (11)$$

- KBR_{N_t} : Kumuliertes Betriebsrisiko im gesamten Netz von Beginn des Kalenderjahrs bis zum Zeitpunkt t (Opfer/Jahr)
- $BR_{B_{n,i}}$: Betriebsrisiko im betrachteten Fdl-Steuerbereich n in der Stunde i (Opfer/Jahr)
- n : Die fortlaufend numerische Kennzeichnung des Fdl-Steuerbereichs im gesamten Netz
- q : Die höchste numerische Kennzeichnung des Fdl-Steuerbereichs, die der Anzahl der Fdl-Steuerbereiche in dem gesamten Netz entspricht
- i : Die fortlaufende Stundenzahl von Beginn des Kalenderjahrs bis zum Zeitpunkt t
- p : Die letzte Stunde der Betrachtung vor dem Zeitpunkt t , die der Anzahl der Stunden von Beginn des Kalenderjahrs bis zum Zeitpunkt t entspricht

3.4.2 Die Struktur der Bewertungssystematik¹⁰

3.4.2.1 Strukturteil - Betriebsszenario

Der Strukturteil Betriebsszenario beinhaltet die Betriebsvariablen sowie die Qualität des aktuellen Betriebsszenarios. Die Betriebsvariablen sind die grundlegenden Eingangsgrößen für die Ableitung der Qualität des Bahnbetriebs bzw. des Rückfallebenenkonzepts eines bestimmten Zeitabschnitts. Bei den Betriebsvariablen wird weiter zwischen den „szenarioübergreifenden Betriebsvariablen“ und „szenariospezifischen Betriebsvariablen“ unterschieden. Die szenarioübergreifenden Betriebsvariablen gelten für alle Betriebsszenarien bzw. Zeitabschnitte in einem Gesamtzeitraum der Betrachtung. Im Gegensatz dazu gelten die szenariospezifischen Betriebsvariablen nur für ein Betriebsszenario bzw. ein Rückfallebenenkonzept in einem bestimmten Zeitabschnitt innerhalb des Gesamtzeitraums.

3.4.2.1.1 Szenarioübergreifende Betriebsvariable

In den szenarioübergreifenden Betriebsvariablen sind die folgenden Variablen enthalten: der Gesamtbereich der Betrachtung und der Gesamtzeitraum der Betrachtung. Mit den szenarioübergreifenden Betriebsvariablen wird die Betrachtungsgrenze einer Bewertung beschrieben. Außerdem ist das Festlegen des Gesamtzeitraums und des Gesamtbereichs die Voraussetzung für die Aufteilung des Risikogrenzwerts des Betriebsrisikos auf den ausgewählten Betrachtungsbereich und die ausgewählte Betrachtungsdauer (siehe Kapitel 3.3.2). Die Details der einzelnen Variablen lauten wie folgt:

- Gesamtbereich der Betrachtung

Mit dieser Variable wird die Größe des gesamten Betrachtungsbereichs beschrieben. Die Größe eines gesamten Betrachtungsbereichs einer Bewertung entspricht dem Steuerbereich eines Fdl. Sind bei einer großräumigen Störung mehrere Fdl-Steuerbereiche betroffen, wird jeder Fdl-Steuerbereich getrennt bewertet, da sich die Variablen zur Abbildung der menschlichen Auslastung auf einen Fdl beziehen. Die Ergebnisse der einzelnen Fdl-Steuerbereiche werden anschließend zur Kontrolle der Risikoentwicklung zusammengefasst. Die Größe eines Steuerbereichs wird durch die Gleislänge im Bereich dargestellt. Bei der Ermittlung der Gleislänge werden lediglich die von Zügen planmäßig befahrenen Gleise bzw. die Hauptgleise berücksichtigt. Nebengleise, die planmäßig nicht von Zügen befahren werden, sind kein Gegenstand der Betrachtung.

- Gesamtzeitraum der Betrachtung

Der Gesamtzeitraum der Betrachtung kann vom Anwender der Bewertungssystematik frei ausgewählt werden. Dieser Zeitraum kann z. B. ein Monat, ein Quartal oder ein Jahr sein. Das Ziel ist, die Betriebsqualität des Bahnbetriebs über einen längeren Zeitraum

¹⁰ Dieser Abschnitt beruht zum Teil auf der autoreigenen Veröffentlichung in [139]

verfolgen und bewerten zu können. In der Bewertungssystematik wird diese Variable benötigt, um die Qualität des Bahnbetriebs mithilfe der entsprechenden Formel in Kapitel 3.4.3 in den Qualitätsindex umrechnen zu können. Außerdem ist auch der Risikogrenzwert im Bereich der Betrachtung von dem Zeitraum der Betrachtung abhängig. In der vorliegenden Arbeit wird der gesamte Zeitraum der Betrachtung gemäß dem Zeitraum der Unfallstatistik auf ein Kalenderjahr festgelegt.

3.4.2.1.2 Szenariospezifische Betriebsvariable

Die szenariospezifischen Betriebsvariablen bilden die Eingangsgröße für die Ermittlung der Betriebsqualität der einzelnen Betriebsszenarien innerhalb eines bestimmten Zeitabschnitts im Gesamtbereich der Betrachtung. Dies beinhaltet insgesamt sieben Variablen zur Beschreibung der Betriebsszenarien im betreffenden Bereich. Dazu gehören der Betriebszustand des Bereichs, die voraussichtliche Dauer des Betriebszustands, die Größe des Bereichs, die Betriebsgeschwindigkeit im Bereich, die Betriebsdichte im Bereich, die Verkehrsart im Bereich und zuletzt die Betriebsweise im Bereich. Die Details der einzelnen Variablen sind wie folgt:

- **Betriebszustand des Bereichs**

Durch diese Variable wird der Gesamtbereich der Betrachtung nach dessen Betriebszustand in Teilbereiche aufgeteilt. Dabei werden drei Betriebszustände berücksichtigt: Regelbetrieb, Störungsbetrieb und Betriebsausfall. Je nach Betriebsszenario oder Rückfallebenenkonzept können im Gesamtbereich der Betrachtung sieben Kombinationen aus Betriebszuständen in einem Zeitabschnitt auftreten. Die sieben Kombinationen aus Betriebszuständen sind:

- Bereich komplett im Regelbetrieb
- Bereich komplett im Störungsbetrieb
- Bereich komplett im Betriebsausfall
- Bereich teils im Regelbetrieb und teils im Betriebsausfall
- Bereich teils im Regelbetrieb und teils im Störungsbetrieb
- Bereich teils im Störungsbetrieb und teils im Betriebsausfall
- Bereich teils im Regelbetrieb, teils im Störungsbetrieb und teils im Betriebsausfall

Der Regelbetrieb ist im Rahmen dieser Arbeit als ein technisch gesicherter Bahnbetrieb ohne Teilnahme von Menschen an sicherheitsrelevanten Handlungen in der normalen Betriebsführung zu verstehen. Im Vergleich zum Regelbetrieb, in dem das Versagen der Menschen im Grunde die Sicherheit des Bahnbetriebs nicht gefährden kann, hat das Versagen der Menschen im Störungsbetrieb mittelbare Auswirkung auf die Sicherheit des Bahnbetriebs. Mindestens eine der sieben Betriebsfunktionen in dem Funktionsmodell (siehe Kapitel 3.4.2.2) wird im Störungsbetrieb vom Menschen als maßgeblicher Akteur übernommen. Der dritte Zustand, der Betriebsausfall, beschreibt einen Stillstand des Bahnbetriebs in einem Bereich / Teilbereich. Im Zeitabschnitt der Betrachtung werden keine Züge durch den Bereich geführt.

- Voraussichtliche Dauer des Betriebsszenarios (ZA_i)

Durch diese Variable wird die voraussichtliche Dauer eines Betriebsszenarios erfasst. Die Betriebsszenarien unterscheiden sich bei der Bewertung im Wesentlichen durch ihre Betriebszustände, die Größen der Bereiche, ihre Funktionsmodelle sowie durch die Verkehrsarten. Im Gegensatz zum Gesamtzeitraum der Betrachtung umfasst die voraussichtliche Dauer des Betriebsszenarios lediglich einen Zeitabschnitt des Gesamtzeitraums. Die Dauer eines Betriebsszenarios wird weiter gezählt, solange dessen Betriebszustand, dessen Größe des Bereichs sowie dessen Funktionsmodell keine Änderung aufweisen. Außerdem gilt die Dauer des Betriebsszenarios für alle Teilbereiche eines Betriebszustandes. Die voraussichtliche Dauer im Störungsbetrieb ist vom Anwender fachlich einzuschätzen.

- Größe des Teilbereichs (GL)

Die Variable Größe des Teilbereichs beschreibt die Gleislänge des Teilbereichs in einem bestimmten Betriebszustand. Die Summe der Gleislängen aller Teilbereiche muss identisch mit der Gleislänge des Gesamtbereichs der Betrachtung sein. Bei der Ermittlung der Größe des Störungsbereichs muss zwischen dem technischen Störungsbereich und dem betrieblichen Störungsbereich differenziert werden. Bei dem Bereich der technischen Störung wird lediglich der Standort oder der Anwendungsbereich des betroffenen technischen Systems betrachtet. Wenn z. B. ein Gleisabschnitt im Stellwerk dauernd besetzt ist dann umfasst der Bereich der technischen Störung nur den einzelnen gestörten Blockabschnitt.

Im Gegensatz zum Bereich der technischen Störung umfasst der Bereich der betrieblichen Störung den gesamten Bereich, in dem sich der Bahnbetrieb im Störungsbetrieb befindet. Wenn z. B. ein Gleisabschnitt im Stellwerk dauernd besetzt ist dann beginnt der Bereich der betrieblichen Störung an der Stelle vor dem gestörten Blockabschnitt, an der der Tf die Fahrerlaubnis für die Durchfahrt des gestörten Blockabschnitts erhält, und endet an der nächsten Räumungsprüfstelle. Ein weiteres Beispiel wäre die Störung eines einzelnen Weichenbereichs. In diesem Fall umfasst der Bereich der technischen Störung lediglich den Bereich der einzelnen gestörten Weiche. Der Bereich der betrieblichen Störung ist deutlich größer und umfasst die gesamte Länge sowie alle zugehörigen Schutzelemente einer Fahrstraße, die für eine sichere Fahrt durch den Bereich benötigt werden.

Bei einer großräumigen Störung können der Bereich der technischen Störung und der Bereich der betrieblichen Störung (nahezu) gleich sein. Wenn z. B. alle Blockabschnitte zwischen zwei Räumungsprüfstellen gestört sind und dauernd besetzt sind dann beginnt der Bereich der betrieblichen Störung am Ausfahrtsignal der ersten Räumungsprüfstelle und endet vor dem Ausfahrtsignal der nächsten Räumungsprüfstelle. In diesem Fall fehlt dem Bereich der technischen Störung zwar der letzte Abschnitt vom Einfahrtsignal bis

zum Ausfahrsignal in der rückliegenden Räumungsprüfstelle, aber im Großen und Ganzen können beide Bereiche bei der Bewertung als identisch betrachtet werden. Eine Gegenüberstellung der Beispiele ist in Tabelle 12 zu finden.

Tabelle 12: Unterschied zwischen dem technischen und betrieblichen Störungsbereich

	Bereich der technischen Störung	Bereich der betrieblichen Störung
Grundsätzliche Unterschiede	Am Standort oder im Anwendungsbereich des betroffenen technischen Systems.	umfasst den gesamten Bereich im Störungsbetrieb, einschließlich des Bereichs der technischen Störung
Beispiel 1: Einzelner Blockabschnitt ist dauernd besetzt	...umfasst nur den einzelnen gestörten Blockabschnitt	...beginnt mit dem Ort vor dem gestörten Blockabschnitt, wo der Tf die Fahrerlaubnis für die Durchfahrt des gestörten Blockabschnittes erhält, bis zur nächsten Räumungsprüfstelle.
Beispiel 2: Einzelner Weichenbereich ist dauernd gestört	...umfasst nur den Bereich der einzelnen gestörten Weiche	...umfasst die gesamte Länge sowie alle zugehörigen Schutzelemente einer Fahrstraße, die für eine sichere Fahrt durch den Bereich benötigt werden
Beispiel 3: Alle Blockabschnitte zwischen zwei Räumungsprüfstellen sind dauernd besetzt	...umfasst alle Blockabschnitte zwischen den zwei Räumungsprüfstellen	...umfasst den Bereich der technischen Störung zzgl. der vor- und nachliegenden Räumungsprüfstellen

- Betriebsgeschwindigkeit (V_B)

Bei der variablen Betriebsgeschwindigkeit handelt es sich um die mittlere Beförderungsgeschwindigkeit im (Teil-)Bereich der Betrachtung. Bei der Ermittlung der Beförderungsgeschwindigkeit werden auch die Haltezeiten berücksichtigt. Daher ist die Beförderungsgeschwindigkeit in der Regel kleiner als die mittlere Fahrgeschwindigkeit des Zuges. Anders als Betriebsdauer und Größe des Bereichs wird diese Variable nur für die Bereiche mit den Betriebszuständen Regelbetrieb und Störungsbetrieb benötigt, da in einem Bereich mit Betriebsausfall keine Fahrten stattfinden.

- Betriebsdichte (D_{AR})

Die Betriebsdichte im (Teil-)Bereich der Betrachtung wird durch die Anzahl der Fahrten pro Stunde im Bereich beschrieben. Bei der Anzahl der Fahrten pro Stunde im Bereich handelt es sich um die mittlere Anzahl der in den Bereich einbrechenden Fahrten, die während der voraussichtlichen Dauer eines Betriebsszenarios in dem (Teil-)Bereich pro Stunde an den Grenzen des Betrachtungsbereichs zu erwarten sind. D. h.: In einem Bereich mit zweigleisigen Strecken und Richtungsbetrieb müssen die einbrechenden Fahrten beider Gleise berücksichtigt werden. Das gleiche gilt auch für eine eingleisige Strecke mit Zweirichtungsbetrieb. Die Betriebsdichte im (Teil-)Bereich der Betrachtung hat daher die Einheit (Fahrten/Std. alle Richtungen)

- Verkehrsart

Durch die Variable Verkehrsart wird allgemein beschrieben, welche Arten von Verkehr im (Teil-)Bereich unterwegs sind. Es sind drei Arten von Verkehr zu unterscheiden, nämlich die Arten Personenverkehr, Güterverkehr oder Mischverkehr. Der Personenverkehr und der Güterverkehr sind artreine Verkehre. Alle Fahrten in einem (Teil-)Bereich sind entweder Reisezüge oder Güterzüge. Der Gegensatz dazu ist der Mischverkehr, in dem die Reisezüge und Güterzüge während der Dauer des Betriebsszenarios auf dem gleichen Streckengleis zu finden sind. Die Differenzierung der Verkehrsart ist entscheidend für die Einschätzung des Schadensausmaßes bei einem Unfall. Das Thema Schadensausmaß verschiedener Verkehrsarten wird im Anschluss in Kapitel 3.4.2.7 behandelt.

- Betriebsweise

Durch die Variable Betriebsweise wird beschrieben, mit welcher Fahrordnung die Fahrten in einem Bereich bzw. auf einem Streckengleis durchgeführt werden. Hier wird zwischen Einrichtungsbetrieb und Zweirichtungsbetrieb unterschieden. Im Einrichtungsbetrieb fahren alle Züge auf einem Streckengleis immer in die gleiche Fahrrichtung, während ein Streckengleis im Zweirichtungsbetrieb wechselnd von Zügen aus entgegengesetzten Richtungen befahren kann. Das Bestimmen der Betriebsweise ist die Voraussetzung für die korrekte Zuweisung der Unfallart, da die Unfallart Frontalzusammenstoß nur im Zweirichtungsbetrieb zu erwarten ist.

3.4.2.2 Strukturteil - Funktionsmodell

Der Strukturteil Funktionsmodell umfasst die generischen Betriebsfunktionen, die für die sichere Durchführung einer Fahrt notwendig sind, und gilt als Basis zur Ermittlung des Betriebsrisikos. Bei der Zusammenstellung des Funktionsmodells wurde die Annahme getroffen, dass jede Betriebsfunktion im Funktionsmodell voneinander unabhängig sein muss. Das bedeutet auch, dass der Bahnbetrieb beim Versagen einzelner Betriebsfunktionen im Funktionsmodell gleich in einen gefährlichen Betriebszustand geführt wird. Für die sichere Durchführung einer Fahrt wurden die vorhandenen Arbeiten in [38, 40, 85, 90] zur Ableitung der generischen Betriebsfunktion herangezogen. Insgesamt wurden sieben generische Betriebsfunktionen aus den vorhandenen Arbeiten identifiziert, die für die sichere Durchführung einer Fahrt maßgeblich sind. Die sieben Betriebsfunktionen sind: Fahrweg sichern, Abstandhaltung sichern, Bahnübergang sichern, Geschwindigkeit signalisieren, Fahrerlaubnis bereitstellen, Fahrt durchführen und Brems- & Antriebskraft bereitstellen.

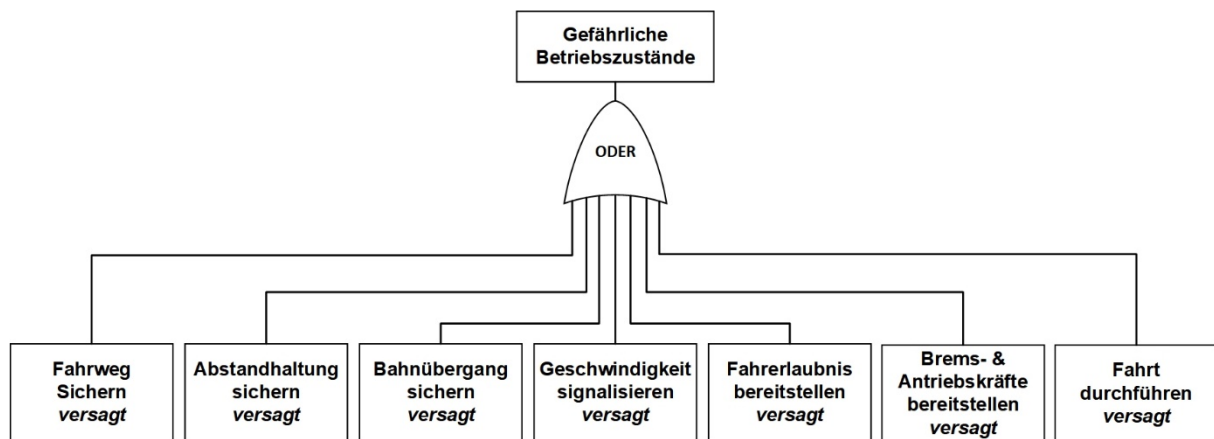


Abbildung 18: Kombination aus Teilfunktionen des Funktionsmodells im Fehlerbaum

Für jede Betriebsfunktion wird ein maßgeblicher Akteur zugeordnet. Der Akteur der Betriebsfunktion ist entweder ein Mensch oder ein technisches System. Ggf. kann eine Betriebsfunktion auch keinen Akteur haben, falls die Betriebsfunktion nicht benötigt wird. Das betrifft vor allem die Betriebsfunktion „Bahnübergang sichern“, da z. B. in Deutschland bei Strecken mit einer Fahrgeschwindigkeit von über 160 km/h kein Bahnübergang erlaubt ist. Wie die Abbildung 18 zeigt, können die Betriebsfunktionen anhand eines Fehlerbaums miteinander kombiniert werden. Aufgrund der Unabhängigkeit zwischen den Betriebsfunktionen werden alle Betriebsfunktionen durch ein „ODER“-Gatter mit dem Hauptereignis des Fehlerbaums „Gefährliche Betriebszustände“ verbunden. Nach der Rechenlogik des Fehlerbaums in [108] kann die Versagensrate des Funktionsmodells, oder auch anders ausgedrückt, das Potenzial, dass der Bahnbetrieb sich in einem gefährlichen Betriebszustand befindet, direkt als Summe der einzelnen Betriebsfunktionen bestimmt werden. Sind aber zugleich Mensch und technisches System als Akteure der Betriebsfunktion in einem Funktionsmodell vorhanden, dann ist eine Umrechnung notwendig, die in Kapitel 3.4.2.4 im Detail behandelt wird.

Jede Betriebsfunktion im Funktionsmodell ist verantwortlich für einen Teil der Sicherheit des Bahnbetriebs und enthält ein eigenes spezifisches Funktionsziel. Die Funktionsziele der sieben Betriebsfunktionen wurden aus den vorhandenen Arbeiten in [38, 40, 85, 90] abgeleitet und zusammengefasst. Eine Übersicht der Betriebsfunktionen und deren Funktionsziel ist am Ende dieses Abschnitts in Tabelle 13 zu finden.

Dies sind die Funktionsziele der jeweiligen Betriebsfunktionen im Einzelnen:

- [F1] Fahrweg sichern

Durch die Betriebsfunktion „Fahrweg sichern“ soll gewährleistet werden, dass die Fahrwegelemente nach dem Einstellen der Fahrstraße für die betreffende Fahrt die richtige Stellung und Endlage haben. Außerdem müssen die richtige Stellung und Endlage der gesicherten Fahrwegelemente solange eingehalten werden, bis die betreffende Fahrt die betreffenden Fahrwegelemente geräumt hat. Im Fall einer falschen Stellung und Endlage der Fahrwegelemente sowie einer vorzeitigen Auflösung oder eines fehlenden Verschlusses von Fahrwegelementen kann es unter Umständen z. B. zur Entgleisung des Eisenbahnfahrzeugs kommen.

- [F2] Abstandhaltung sichern

Durch die Betriebsfunktion „Abstandhaltung“ soll gewährleistet werden, dass Fahrweg, Durchrutschweg und Flankenschutzraum für die betreffende Fahrt weder von einem Fahrzeug besetzt noch von einer Folgefahrt, Gegenfahrt oder Flankenfahrt beansprucht werden. Außerdem müssen die vorstehend genannten Bedingungen „Abschnitt ist frei und wird nicht beansprucht“ solange eingehalten werden, bis die betreffende Fahrt die betreffenden Gleisabschnitte geräumt hat. Im Fall einer fehlerhaften Ergebnismeldung, z. B. Abschnitt ist besetzt, wird aber als frei gemeldet, sowie eines fehlerhaften Ausschlusses von Folgefahrten, Gegenfahrten oder Flankenfahrten kann es unter Umständen zum Zusammenstoß zwischen den Eisenbahnfahrzeugen kommen.

- [F3] Bahnübergang sichern

Durch die Betriebsfunktion „Bahnübergang sichern“ soll gewährleistet werden, dass der Bahnübergang zur Durchführung der betreffenden Fahrt gesichert ist. Im Fall eines ungesicherten Bahnübergangs bei der Durchführung der Fahrten kann es unter Umständen zum Zusammenprall zwischen dem Eisenbahnfahrzeug und einem Straßenverkehrsteilnehmer führen. Diese Betriebsfunktion ist jedoch optional, da nicht auf allen Strecken ein Bahnübergang vorhanden ist.

- [F4] Fahrerlaubnis bereitstellen

Durch die Betriebsfunktion „Fahrerlaubnis bereitstellen“ soll gewährleistet werden, dass die Fahrerlaubnis erst erteilt wird, wenn die Voraussetzungen für das Erteilen einer Fahrerlaubnis erfüllt sind. Es wird sichergestellt, dass der Inhalt der Fahrerlaubnis und der Zeitpunkt der Erteilung der Fahrerlaubnis korrekt sind sowie der Vorgang der Erteilung der Fahrerlaubnis korrekt durchgeführt wird. Vor der Erteilung einer

Fahrerlaubnis müssen die Zustände der Betriebsfunktionen „Fahrweg sichern“, „Abstandhaltung sichern“ und „Bahnübergang sichern“ als Bedingungen geprüft werden. Im Fall einer fehlerhaften Fahrerlaubnis sowie einer unzeitigen Erteilung der Fahrerlaubnis kann es unter Umständen z. B. zur Entgleisung des Eisenbahnfahrzeugs, zum Zusammenstoß zwischen den Eisenbahnfahrzeugen oder zum Zusammenprall mit einem Straßenverkehrsteilnehmer kommen.

- [F5] Geschwindigkeit signalisieren

Durch die Betriebsfunktion „Geschwindigkeit signalisieren“ soll gewährleistet werden, dass die für den Fahrtverlauf zulässige Geschwindigkeit, einschließlich der zugbezogenen, streckenbezogenen sowie fahrstraßenabhängigen Geschwindigkeit, korrekt signalisiert bzw. vermittelt wird. Im Fall einer fehlerhaften Geschwindigkeitssignalisierung bzw. -vermittlung kann es unter Umständen z. B. zur Entgleisung des Eisenbahnfahrzeugs, zum Zusammenstoß zwischen den Eisenbahnfahrzeugen oder zum Aufprall eines Eisenbahnfahrzeugs auf den Gleisabschluss kommen. An dieser Stelle ist Folgendes zu beachten: Eine zulässige Geschwindigkeit, deren Ursprung auf die Reduzierung des Schadensausmaßes bei der Durchführung von Fahrten im Störungsbetrieb zurückzuführen ist, also z. B. Fahren auf Sicht im Kombination mit der Räumungsprüfung, wird im Rahmen dieser Arbeit nicht als die Betriebsfunktion „Geschwindigkeit signalisieren“ angesehen, sondern wird zu dem Inhalt der Betriebsfunktion „Fahrerlaubnis bereitstellen“ zugeordnet.

- [F6] Brems- & Antriebskräfte bereitstellen

Durch die Betriebsfunktion „Brems- & Antriebskräfte bereitstellen“ soll gewährleistet werden, dass die Brems- und Antriebskräfte eines Eisenbahnfahrzeugs während der Durchführung der betreffenden Fahrt korrekt funktionieren. Im Fall einer unzureichenden Bremskraft oder einer übermäßigen Antriebskraft kann es unter Umständen z. B. zur Entgleisung des Eisenbahnfahrzeugs, zum Zusammenstoß zwischen den Eisenbahnfahrzeugen oder zum Aufprall eines Eisenbahnfahrzeugs auf den Gleisabschluss kommen.

- [F7] Fahrt durchführen

Durch die Betriebsfunktion „Fahrt durchführen“ soll gewährleistet werden, dass die betreffende Fahrt in den betreffenden Gleisabschnitten vom Beginn bis zum Ende des gesamten Fahrtverlaufs korrekt durchgeführt wird. Es wird berücksichtigt, ob der maßgebliche Akteur die ihm vorliegende gültige Fahrerlaubnis und Geschwindigkeitsinformation richtig interpretiert und korrekt ausgeführt hat. Im Fall einer fehlerhaften Interpretation der Fahrerlaubnis oder der Geschwindigkeitsinformation sowie einer fehlerhaften Ausführung kann es unter Umständen z. B. zur Entgleisung des Eisenbahnfahrzeugs, zum Zusammenstoß zwischen den Eisenbahnfahrzeugen, zum Aufprall eines Eisenbahnfahrzeugs auf den Gleisabschluss oder zum Zusammenprall mit einem Straßenverkehrsteilnehmer kommen. Bei der Identifizierung des maßgeblichen

Akteurs der Betriebsfunktion „Fahrt durchführen“ werden folgende Regeln berücksichtigt:

- Das technische System ist der maßgebliche Akteur der Betriebsfunktion „Fahrt durchführen“:
 - Wenn die Fahrten vom Start bis zum Stopp automatisch durch Technik durchgeführt werden. Das entspricht einem Bahnbetrieb mit z. B. einem Automatisierungsgrad (GoA) von GoA-2 (Halbautomatischer Fahrbetrieb)¹¹, GoA-3 (Fahrerloser Fahrbetrieb)¹² oder GoA-4 (Unbegleiteter Fahrbetrieb)¹³ nach DIN EN 62267 [109]
 - Wenn die Fahrten manuell vom Menschen gesteuert, aber unter der Überwachung und Einwirkung einer technischen Sicherung durchgeführt werden. Allerdings ist der Mensch bei der betroffenen Fahrt nicht berechtigt, die technische Überwachung und Einwirkung der Zugbeeinflussung zu unterdrücken. Abgesehen von einer absichtlichen Handlung bedeutet das: Solange der Mensch nicht durch irgendeine Weise berechtigt wurde, die technische Sicherung bei der betroffenen Fahrt unter bestimmten Betriebszuständen unterdrücken zu dürfen, ist die Fahrt technisch gesichert. Dadurch wird die Technik in diesem Fall als der maßgebliche Akteur der Betriebsfunktion angesehen.
- Der Mensch ist der maßgebliche Akteur der Betriebsfunktion „Fahrt durchführen“:
 - Wenn die Fahrten manuell vom Menschen gesteuert, aber unter der Überwachung und Einwirkung der technischen Sicherung durchgeführt werden. Allerdings wurde, egal ob regelkonform nach Eigenentscheidung des Tf oder nach dem Befehl einer leitenden Stelle, der Mensch bei der betreffenden Fahrt berechtigt, die Einwirkung der Zugbeeinflussung während der Durchführung der Fahrt unter den bestimmten Betriebszuständen unterzudrücken. Das bedeutet: Falls z. B. der Tf durch den Befehl berechtigt wurde, die Einwirkung der Zugbeeinflussung zum Vorbeifahren an einem haltzeigenden Hauptsignal zu unterdrücken, dann

¹¹ Bei GoA-2 (STO) handelt es sich nach [109] um einen halbautomatisierten Bahnbetrieb, in dem die Fahrt vom Start bis zum Stopp automatisch durch Technik durchgeführt wird. Der Start wird zwar noch von dem Tf ausgelöst, ist aber nicht sicherheitsrelevant.

¹² Bei GoA-3 (DTO) handelt es sich nach [109] um einen fahrerlosen automatisierten Bahnbetrieb, der nur noch einen Zugbegleiter hat. Der Zugbegleiter ist bei der Durchführung von Fahrten im Regelbetrieb nicht involviert.

¹³ Bei GoA-4 (UTO) handelt es sich nach [109] um einen vollautomatisierten fahrerlosen Bahnbetrieb, bei dem sich keine Bedienstete im Fahrzeug befindet. Im Störungsbetrieb kann der Zugbetrieb automatisch weiter durchgeführt werden oder der Bedienstete in der Leitzentrale kann auch in den Zugbetrieb eingreifen.

ist der Mensch (Tf) in dieser Fahrt der maßgebliche Akteur der Betriebsfunktion.

- Wenn die Fahrten manuell von dem Menschen gesteuert und teils oder komplett ohne die technische Überwachung und Einwirkung der technischen Sicherung durchgeführt werden.

Tabelle 13: Betriebsfunktionen des Funktionsmodelles und deren Funktionsziele

Betriebsfunktion	Funktionsziel
[F1] Fahrweg sichern	gewährleistet, dass die Fahrwegelemente nach dem Einstellen der Fahrstraße für die betreffende Fahrt die richtige Stellung und Endlage haben. Außerdem müssen die vorstehend genannten Bedingungen solange eingehalten werden, bis die betreffende Fahrt die Fahrwegelemente geräumt hat.
[F2] Abstandhaltung sichern	gewährleistet, dass Fahrweg, Durchrutschweg und Flankenschutzraum für die betreffende Fahrt weder von einem Fahrzeug besetzt noch von einer Folgefahrt, Gegenfahrt oder Flankenfahrt beansprucht werden. Außerdem müssen die vorstehend genannten Bedingungen solange eingehalten werden, bis die betreffende Fahrt die betreffenden Gleisabschnitte geräumt hat.
[F3] Bahnübergang sichern	gewährleistet, dass der Bahnübergang zur Durchführung der betreffenden Fahrt gesichert ist
[F4] Fahrerlaubnis bereitstellen	gewährleistet, dass der Fahrerlaubnis erst erteilt wird, wenn die Voraussetzungen für das Erteilen einer Fahrerlaubnis erfüllt sind.
[F5] Geschwindigkeit signalisieren	gewährleistet, dass die für den Fahrtverlauf zulässige Geschwindigkeit, einschließlich der zugbezogenen, der streckenbezogenen sowie der fahrstraßenabhängigen Geschwindigkeit, korrekt signalisiert bzw. vermittelt wird.
[F6] Brems- & Antriebskräfte bereitstellen	gewährleistet, dass die Brems- und Antriebskräfte bei der Durchführung der betreffenden Fahrt korrekt funktionieren.
[F7] Fahrt durchführen	gewährleistet, dass die betreffende Fahrt vom Beginn bis zum Ende des gesamten Fahrtverlaufs in den betreffenden Gleisabschnitten korrekt durchgeführt wird.

3.4.2.3 Strukturteil - Versagenspotenzial

Nachdem das Betriebsszenario beschrieben sowie die Betriebsfunktionen in dessen Funktionsmodell dem entsprechenden Akteur zugeordnet wurden, folgt die Bestimmung des Versagenspotenzials des Funktionsmodells als nächster Schritt unter der Gegebenheit des vorliegenden Betriebsszenarios. Bei der Bestimmung des Versagenspotenzials eines Funktionsmodells, das ausschließlich das technische System als maßgeblichen Akteur hat, kann die Versagensrate der einzelnen Betriebsfunktionen direkt miteinander addiert werden. Bei einem Funktionsmodell, in dem mindestens eine der sieben Betriebsfunktionen in einem Störungsbetrieb vom Menschen als maßgeblicher Akteur übernommen wird, ist eine Ableitung des Versagenspotenzials wegen der unterschiedlichen Einheiten der technischen Versagensrate (Versagen/Zeiteinheit) und der menschlichen Versagenswahrscheinlichkeit (einheitslos) nicht direkt möglich. Aus diesem Grund muss das Versagenspotenzial eines Funktionsmodells in dieser Phase nach dessen Akteur getrennt bestimmt werden. Das Versagenspotenzial eines Funktionsmodells wird erst durch eine Umrechnungslogik in der nächsten Phase der Bewertung „Anzahl der Versagen“ zusammengefasst. Aus der generischen Betrachtung kann der maßgebliche Akteur einer Betriebsfunktion entweder ein technisches System oder ein Mensch sein. Beim Menschen wird weiterhin nach Fahrdienstleiter, der in der Regel für die Tätigkeit „Sichern der Fahrt“ im Störungsbetrieb zuständig ist, und nach Triebfahrzeugführer, der in der Regel für die Tätigkeit „Durchführen der Fahrt“ im Störungsbetrieb verantwortlich ist, unterschieden. Letztendlich wird das Versagenspotenzial eines Funktionsmodells nach dessen maßgeblichem Akteur der Betriebsfunktion in die folgenden drei maßgeblichen Akteure aufgeteilt und getrennt behandelt: Technik, Fdl und Tf, wie die Abbildung 19 zeigt.

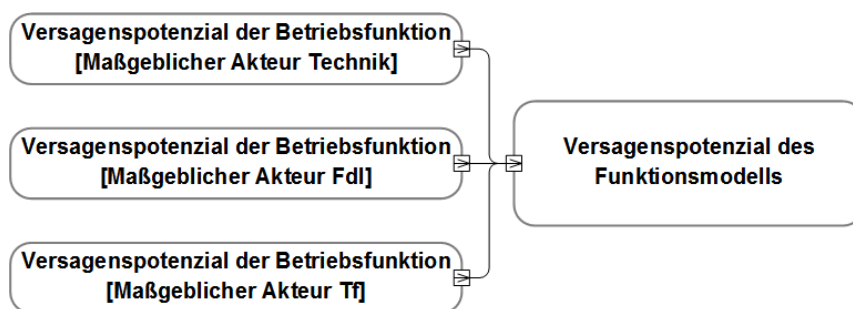


Abbildung 19: Unterteilung des Versagenspotenzials nach dessen maßgeblicher Akteur

3.4.2.3.1 Versagenspotenzial Akteur Technik

Das Versagenspotenzial des Akteurs Technik umfasst die Summe der Versagensrate aller Betriebsfunktionen, die die Technik als maßgeblichen Akteur haben, wie die Abbildung 20 zeigt. Die Versagensrate eines technischen Systems muss bereits vor der Inbetriebnahme nachgewiesen werden. Anders als die Versagenswahrscheinlichkeit des Menschen ist eine szenariobedingte Anpassung der Versagensrate im laufenden Betrieb nicht notwendig und auch nicht vorgesehen. Zur detaillierten Angabe der Versagensrate einer durch die Technik realisierten Betriebsfunktion können, sofern verfügbar, z. B. die Designunterlagen des

technischen Systems herangezogen werden. Andernfalls kann die Vorgabe der Norm referenziert werden, z. B. in Deutschland die DIN VDE V 0831-103 für die Sicherheitsanforderungen an die technischen Funktionen in der Signaltechnik.

Grundsätzlich ist eine derartig genaue Angabe der Versagensrate auf der Ebene der generischen Betriebsfunktion und auch zum Zweck der schnellen Entscheidungsfindung im Störungsbetrieb nicht zwingend notwendig. Auf dieser Abstraktionsebene kann z. B. angenommen werden, dass beim Versagen einer technisch realisierten Betriebsfunktion im Funktionsmodell mit einer unmittelbaren katastrophalen Folge zu rechnen ist. Dadurch kann bei der Versagensrate der technischen Systeme in Europa auf z. B. die Anforderung der CSM-Verordnung [20] verwiesen werden. Dort wird wie folgt beschrieben: *„Bei technischen Systemen, bei denen im Falle eines funktionellen Ausfalls von unmittelbaren katastrophalen Folgen auszugehen ist, muss das damit verbundene Risiko nicht weiter eingedämmt werden, wenn die Ausfallrate pro Betriebsstunde kleiner oder gleich $1E-09$ ist.“* Dadurch kann die Versagensrate jeder Betriebsfunktion mit dem höchsten Niveau der Sicherheitsanforderung $1E-09$ Versagen/Betriebsstunde näherungsweise angenommen werden. Aufgrund der fehlenden Daten der genauen Ausfallrate soll die folgende Berechnung nur beispielhaft zeigen, wie der Ansatz anzuwenden ist. Das Versagenspotenzial des Akteurs Technik ergibt sich dann aus der Summe der Versagensrate der einzelnen Betriebsfunktionen. Dadurch kann z. B. für ein Funktionsmodell bei einem technisch gesicherten Regelbetrieb in allen sieben Betriebsfunktionen ein Versagenspotenzial von $7E-09$ Versagen/Betriebsstunde eingeschätzt werden.

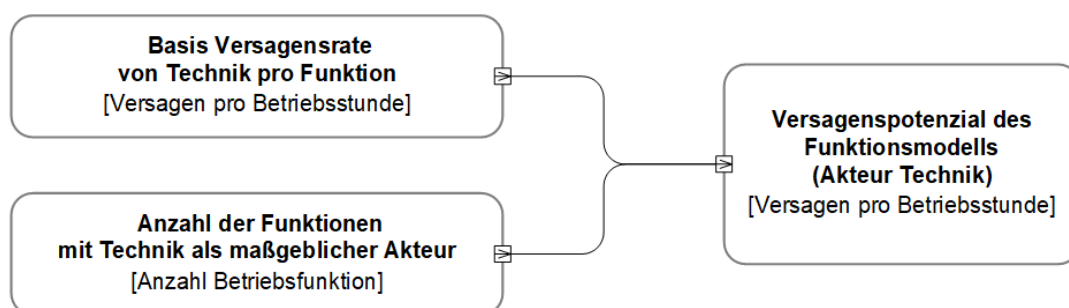


Abbildung 20: Konzept des Versagenspotenzials eines Funktionsmodells von Akteur Technik

3.4.2.3.2 Versagenspotenzial Akteur Fahrdienstleiter

Das Versagenspotenzial des Akteurs Fahrdienstleiter beinhaltet die Versagenswahrscheinlichkeit aller Betriebsfunktionen, die den Fdl als maßgeblichen Akteur haben. Außer bei den Betriebsfunktionen [F6] Bremse- & Antriebskräfte bereitstellen sowie [F7] Fahrt durchführen kann der Fdl im heutigen System in der Regel als maßgeblicher Akteur zugeordnet werden. Technisch zwar möglich, aber noch nicht weit verbreitet ist, dass die Durchführung der Fahrt durch den Fdl von der Leitstelle aus ferngesteuert wird. In diesem Fall kann die Betriebsfunktion [F7] Fahrt durchführen auch zu der Tätigkeit des Fdl zugeordnet werden. Die Versagenswahrscheinlichkeit des Fdl kann, wie in Kapitel 3.1.3 beschrieben, im Fall einer Störung durch folgende drei Faktoren beeinflusst werden: die Dauer der Handlung,

der Umfang der Handlung sowie die Intensität der Handlung. Anders als die technische Versagensrate, für welche keine Anpassung im laufenden Betrieb vorgesehen wird, wird die Versagenswahrscheinlichkeit des Menschen nach der Gegebenheit des aktuellen / voraussichtlichen Betriebsszenarios auslastungsbedingt im laufenden Betrieb angepasst.

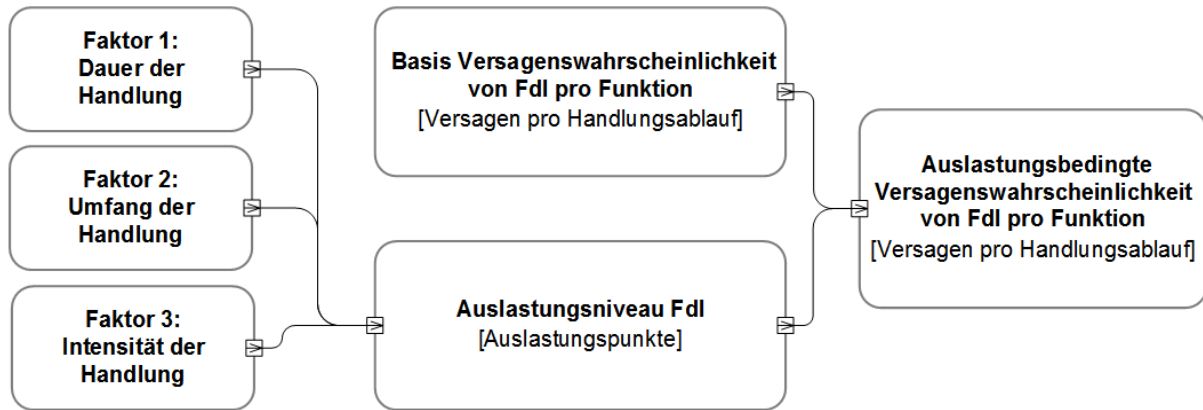


Abbildung 21: Konzept der auslastungsbedingte Versagenswahrscheinlichkeit des Fdl

Wie die Abbildung 21 zeigt, wird die auslastungsbedingte Versagenswahrscheinlichkeit des Fdl ausgehend von einer ausgewählten Basis-Versagenswahrscheinlichkeit im Zusammenhang mit dem aktuellen / voraussichtlichen Auslastungsniveau der Fdl abgeleitet. Zum Festlegen der Basis-Versagenswahrscheinlichkeit des Menschen kann in Deutschland z. B. auf die Arbeit von Hinzen [77] referenziert werden. Die Arbeit von Hinzen wird seit den 1990er Jahren in Deutschland weitverbreitet angewendet, die zur Risikoanalyse ebenfalls als Stand der Technik vom Eisenbahnbundesamt (EBA) akzeptiert wurde [89]. Laut der Arbeit von Hinzen hat der Mensch eine Versagenswahrscheinlichkeit von $1E-03$ bei einer fertigkeitsbasierten Handlung unter einem optimalen Stressniveau und günstigen Arbeitsbedingungen. Allerdings wird diese Versagenswahrscheinlichkeit häufig als zu konservativ kritisiert. Bei einer Versagenswahrscheinlichkeit von $1E-03$ würde das bedeuten, dass bei je 1000 menschlichen Handlungen einmal ein gefährliches Versagen erwartet wird. Der Mensch, z. B. der Fdl, begeht aber in der Realität weniger Fehler, als bei der Quantifizierung von Hinzen angegeben wurde. Wie in [110] beschrieben: „[...] dass der Mensch in der Realität weniger Fehler macht, als sich bei der einfachen Quantifizierung ergeben würden. Das wird dadurch begründet, dass die meisten Handlungen des Bedienpersonals Handlungsabläufe sind und damit aus mehreren Schritten bestehen. [...] Auf diese Art lassen sich Wahrscheinlichkeiten für Fehlhandlungen in der Größenordnung von bis zu $1E-6$ pro Handlungsablauf erreichen“. Das bedeutet, dass die Basis-Versagenswahrscheinlichkeit pro Handlungsablauf mit $1E-06$ eingeschätzt werden kann. Angesichts der Generalität der Betriebsfunktionen in dem Funktionsmodell wird im Rahmen dieser Arbeit angenommen, dass die Ausführung einer Betriebsfunktion von einem menschlichen Akteur als ein Handlungsablauf betrachtet wird. Wie die Abbildung 22 zeigt, werden in der Ausführung alle Teilschritte einer Betriebsfunktion als ein Handlungsablauf zusammengefasst, unabhängig von der Anzahl der Teilnehmer. Diese Annahme hat auch Auswirkung auf den Einflussfaktor der menschlichen Auslastung „Intensität der Handlung“.

Da die Teilschritte des Handlungsablaufs nicht mehr berücksichtigt werden, kann die Anzahl der Teilschritte auch keinen Einfluss auf die Intensität der Handlung haben. Die Intensität der Handlung wird dann von den Variablen Größe des Bereichs, der Betriebsdichte und der Betriebsgeschwindigkeit abhängig gemacht.

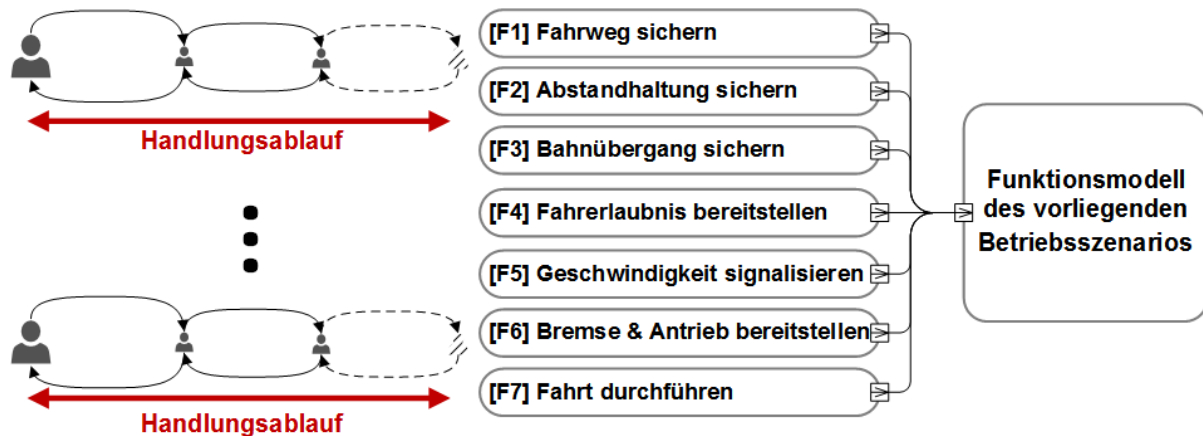


Abbildung 22: Konzept eines Handlungsablaufs

Nachdem die Basis-Versagenswahrscheinlichkeit ausgewählt wurde, muss vor dem Ableiten der auslastungsbedingten Versagenswahrscheinlichkeit noch das Auslastungsniveau des Fdl im Störungsbetrieb bestimmt werden. Zur Ermittlung des Auslastungsniveaus werden drei Einflussfaktoren, nämlich die Dauer der Handlung, der Umfang der Handlung und die Intensität der Handlung, zusammenhängend berücksichtigt. Die Werte des jeweiligen Einflussfaktors werden durch die logarithmische Transformation in eine logarithmierte Punkteskala verwandelt. Das Auslastungsniveau des Fdl ergibt sich dann aus der Punktesumme des jeweiligen Einflussfaktors und ggf. mit Gewichtung zwischen den Faktoren. Die logarithmische Transformation dient dem Zweck, den Einfluss der extremen Werte eines einzelnen Faktors, welcher eine deutlich größere Skalenbreite hat, auf das Ergebnis des Auslastungsniveaus zu minimieren. Ohne diese Transformation kann die Wertänderung eines Faktors, welcher nur eine kleine Skalenbreite hat, keinen oder nur minimalen Einfluss auf das Ergebnis haben, wenn die Punktesumme eines anderen Faktors mit einem deutlich höheren Wert dominiert wird. Um die kleine Änderung der Einflussfaktoren und deren Auswirkung auf das Ergebnis möglichst genau darstellen zu können, wird bei der Transformation die logarithmische Basis von ca. $\sqrt{3}$ ausgewählt, welche auch der Bandbreite der Variablen entspricht. Das bedeutet auch: Wenn die Punktesumme des Auslastungsniveaus um einen Punkt ansteigt, wird die Versagenswahrscheinlichkeit des Fdl pro Handlungsablauf um ca. Faktor $\sqrt{3}$ erhöht.

Die Details der drei Einflussfaktoren sind wie folgt:

Faktor 1: Dauer der Handlung

Durch den Faktor Dauer der Handlung wird der Anstieg der aktiven Arbeitszeit im Störungsbetrieb auf die Auslastung des Fdl berücksichtigt. Hier ist zu beachten, dass die Dauer der Handlung im Störungsbetrieb nicht mit der gesamten Schichtzeit des Fdl zu verwechseln

ist. Bei der Schichtzeit des Fdl handelt es sich um die reguläre Arbeitszeit eines Fdl pro Schicht, die je nach Frühschicht, Spätschicht, Nachtschicht oder Sonn- und Feiertagschicht zwischen 6 und 12 Std. liegen kann. Anders als die Schichtzeit der Arbeit werden bei dem Faktor Dauer der Handlung lediglich die aufeinanderfolgenden Zeiten im Störungsbetrieb berücksichtigt, in den der Fdl aktiv in die sicherheitsrelevanten Handlungen eingebunden ist. Die Dauer der Handlung kann deshalb nur kleiner als oder gleich der Schichtzeit sein. Der obere Grenzwert der Dauer der Handlung ist nach der gesetzlichen Vorgabe anzusetzen. In Deutschland kann der Grenzwert der Arbeitszeit pro Schicht z. B. nach dem Arbeitsgesetz auf 12 Stunden angesetzt werden [111]. Eine voraussichtliche Dauer der Handlung von 12 Std. hat die Bedeutung, dass ein Fdl während seiner 12 Stunden Schichtzeit mindestens 11 Stunden, max. aber bis zu 12 aufeinanderfolgenden Stunden im Störungsbetrieb aktiv mit den sicherheitsrelevanten Handlungen tätig sein wird. Die kontinuierliche Stundenangabe der Dauer der Handlung zwischen 1 und 12 Std. wird nach der Transformation in eine Punkteskala mit fünf Klassen bzw. Auslastungsniveaus umgewandelt, wie die Tabelle 14 zeigt. Die höchste Klasse bzw. das höchste Auslastungsniveau mit dem Punktestand 5 umfasst alle Stundenangaben, die über 8 Stunden hinausgehen. Dies hat die Bedeutung, dass die Dauer einer Handlung zwischen 8 und 12 Stunden den gleichen Einfluss auf das Auslastungsniveau des Fdl hat. Die Auslastungskurve widerspricht dann in diesem Bereich der Kenntnis eines exponentiell steigenden Auslastungsverlaufs mit dem Anstieg der Arbeitszeiten. Das wird damit begründet, dass die Schichtarbeit, deren Schichtzeit über reguläre 8 Stunden hinausgeht, besonderen Regelungen des Arbeitsgesetzes entsprechen muss. Daher wird angenommen, dass die zusätzliche Auslastung des Fdl in höheren Stundenbereichen durch die organisatorischen Maßnahmen ausgeglichen wird.

Tabelle 14: Punkteskala Faktor 1 – Dauer der Handlung

Dauer der Handlung	Transformieren	Punkteskala	Rundungsfehler
h	$\log_{\sqrt[3]{3}} h + 1$	Runden ($\log_{\sqrt[3]{3}} h + 1$)	Δ (Punkteskala - Transformieren)
1	1,00	1	0,00
2	2,20	2	-0,20
3	2,91	3	0,09
4	3,41	3	-0,41
5	3,80	4	0,20
6	4,11	4	-0,11
7	4,38	4	-0,38
8	4,61	5	0,39
9	4,82	5	0,18
10	5,00	5	0,00
11	5,17	5	-0,17
12	5,32	5	-0,32

Faktor 2: Umfang der Handlung

Durch den Faktor Umfang der Handlung wird der Anstieg der Anzahl der Betriebsfunktionen, zu denen der Fdl als maßgeblicher Akteur zugeordnet wurde, auf die Auslastung des Fdl berücksichtigt. Hier wird angenommen, dass jede Betriebsfunktion die gleiche Auslastung auf den Fdl hat. Außer zu der Betriebsfunktion [F6] Bremse-&Antriebskräfte bereitstellen kann der Fdl als maßgeblicher Akteur allen Betriebsfunktionen zugeordnet werden. Wie in Tabelle 15 dargestellt ist, wird die Anzahl der Betriebsfunktionen nach der Transformation in eine Punkteskala mit vier Klassen bzw. Auslastungsniveaus umgewandelt.

Tabelle 15: Punkteskala Faktor 2 – Umfang der Handlung

Anzahl der Betriebsfunktion	Transformieren	Punkteskala	Rundungsfehler
u	$\log_{\sqrt{3}} u + 1$	Runden ($\log_{\sqrt{3}} u + 1$)	Δ (Punkteskala - Transformieren)
1	1,00	1	0,00
2	2,20	2	-0,20
3	2,91	3	0,09
4	3,41	3	-0,41
5	3,80	4	0,20
6	4,11	4	-0,11
Zusätzliche Aufgaben vom Fdl, wie Zuglaufverfolgung, die außerhalb des Funktionsmodells liegt, werden pauschal mit +1 Punkteskala betrachtet, sofern es zutrifft.			

Zusätzlich wird berücksichtigt, dass der Fdl im Störungsbetrieb neben den sicherheitsrelevanten Betriebsfunktionen eventuell auch zusätzliche Aufgaben durchzuführen hat, z. B. die Zuglaufverfolgung beim Ausfall der Zugnummernmeldeanlagen. Alle zusätzlichen Aufgaben vom Fdl im Störungsbetrieb, die nicht im Funktionsmodell abgebildet wurden, werden pauschal mit +1 Punkt in der Punkteskala berücksichtigt, sofern dies zutrifft.

Faktor 3: Intensität der Handlung

Durch den Faktor Intensität der Handlung wird der Anstieg der Ausführungsfrequenz des Funktionsmodells auf die Auslastung des Fdl berücksichtigt. Wie in Kapitel 3.4.2.2 beschrieben, umfasst ein Funktionsmodell die generischen Betriebsfunktionen, die für die sichere Durchführung einer Fahrt von A nach B benötigt werden. Das bedeutet, dass die Ausführung eines Funktionsmodells als die Durchführung einer Fahrt von A nach B angesehen werden kann. Die Ausführung der Betriebsfunktionen im Zusammenhang mit der Durchführung einer Fahrt von A nach B wird hier mit dem Begriff „Funktionsablauf“ bezeichnet. Mit dem Anstieg der Anzahl von Funktionsabläufen innerhalb eines bestimmten Zeitabschnitts, steigt auch die Intensität der Handlung bzw. die Auslastung des Fdl entsprechend. Das Konzept Funktionsablauf ist außerdem die Basis der Umrechnungslogik, mit der das Versagenspotenzial der technischen und menschlichen Akteure später im Strukturteil Anzahl der Versagen zusammengeführt werden kann. Das Konzept kann hier mit Hilfe der Darstellung in Abbildung 23 erklärt werden.

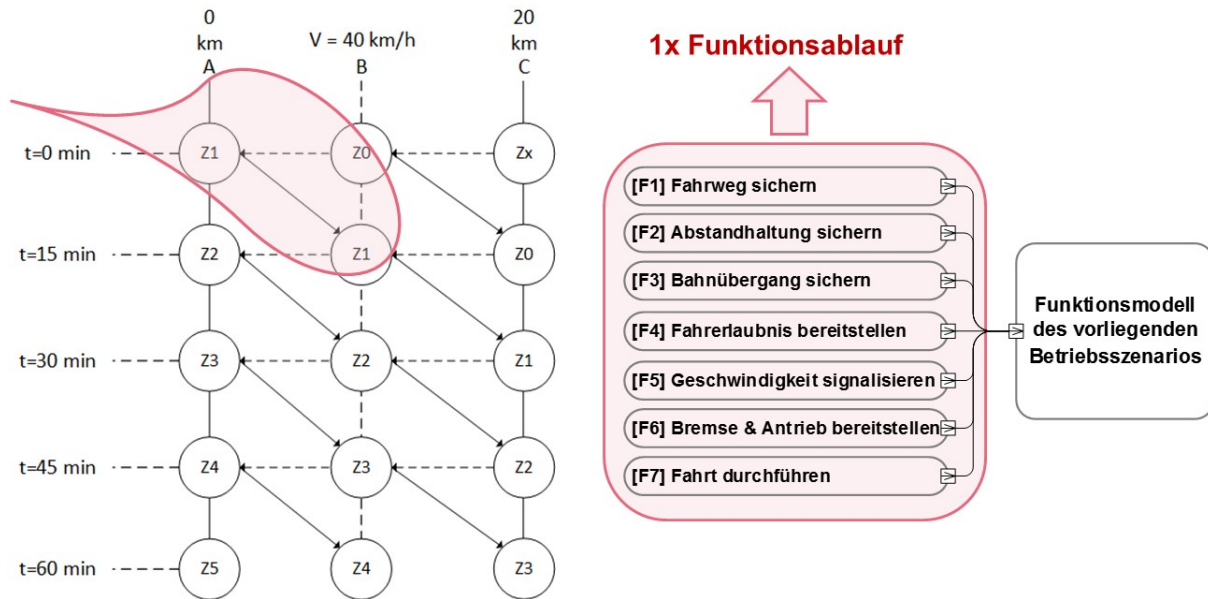


Abbildung 23: Konzept eines Funktionsablaufs

Wie die Abbildung 23 zeigt, ist eine Zugfahrt $Z_{1(A \rightarrow B)}$ von A nach B durchzuführen. Bevor jedoch die Zugfahrt $Z_{1(A \rightarrow B)}$ stattfinden kann, muss durch die Betriebsfunktion [F2] (Abstandhaltung sichern) sichergestellt werden, dass der Abschnitt A-B tatsächlich frei ist. D. h., dass der vorausfahrende Zug Z_0 in B vollständig angekommen und gegen Anfahren, z. B. durch ein „Halt“ zeigendes Hauptsignal, geschützt ist. Außerdem muss sichergestellt werden, dass der Abschnitt A-B nicht von einer anderen Fahrt beansprucht wird. Darüber hinaus muss die richtige Stellung und Endlage der beweglichen Fahrwegelemente im Fahrweg durch die Betriebsfunktion [F1] (Fahrweg sichern) sichergestellt werden. Ist ein Bahnübergang im Abschnitt vorhanden, ist dieser durch die Betriebsfunktion [F3] (Bahnübergang sichern) entsprechend zu sichern. Anschließend wird durch die Betriebsfunktion [F4] (Fahrerlaubnis bereitstellen) sichergestellt, dass alle Voraussetzungen für die Erteilung der Fahrerlaubnis für eine Fahrt von A nach B erfüllt sind. Im Fall einer positiven Kontrollprüfung kann die Fahrerlaubnis erteilt werden und es muss sichergestellt werden, dass der Vorgang der Erteilung der Fahrerlaubnis korrekt durchgeführt wird. Während der Fahrt muss die zulässige Geschwindigkeit durch die Betriebsfunktion [F5] (Geschwindigkeit signalisieren) zur Verfügung gestellt werden. Ebenfalls sind funktionierende Brems- & Antriebskräfte durch die Betriebsfunktion [F6] (Bremse & Antrieb bereitstellen) für die Durchführung der Fahrt bereitzustellen. Die Zugfahrt $Z_{1(A \rightarrow B)}$ ist dann durch die Betriebsfunktion [F7] (Fahrt durchführen) korrekt auszuführen. Der Verlauf eines Funktionsablaufs endet mit der Ankunft des Z_1 in B und der Auflösung der zugehörigen Betriebsfunktionen. Für die nächste Zugfahrt $Z_{2(A \rightarrow B)}$ ist der gleiche Verlauf des Funktionsablaufs zu wiederholen.

Das Beispiel in Abbildung 23 zeigt: Um im Störungsbetrieb einen 15-Minuten-Takt auf einer Strecke von 20 km Länge mit einer Beförderungsgeschwindigkeit von 40 km/h realisieren zu können, werden für jede Zugfahrt zwei Funktionsabläufe benötigt: einmal im Abschnitt A-B und das zweite Mal im Abschnitt B-C. Wird die Taktzeit auf 30 Minuten verlängert, fallen nach

dem Beispiel die Zugfahrten $Z_{2(A \rightarrow C)}$ und $Z_{4(A \rightarrow C)}$ zwischen Abschnitt A und C aus. Der zweite Funktionsablauf von $Z_{1(B \rightarrow C)}$ war im 15-Minuten-Takt notwendig, damit die $Z_{2(A \rightarrow B)}$ um Minuten $t=15$ stattfinden kann. Da jetzt die $Z_{2(A \rightarrow C)}$ ausfällt und der Funktionsablauf von $Z_{3(A \rightarrow C)}$ erst um Minuten $t=30$ beginnt, ist der zweite Funktionsablauf $Z_{1(B \rightarrow C)}$ im 30-Minuten-Takt theoretisch nicht mehr nötig. Für die Zugfahrt $Z_{1(A \rightarrow C)}$ wird im 30-Minuten-Takt nur ein Funktionsablauf zwischen Abschnitt A und C benötigt. Durch diese Logik kann die Anzahl der Funktionsabläufe pro Zugfahrt durch den Störungsbereich in Abhängigkeit von der Streckenlänge im Störungsbereich (SL_{SB}), der mittleren Beförderungsgeschwindigkeit im Störungsbereich (V_B) und der mittleren Taktzeit im Störungsbereich (T_{SR}) eingeschätzt werden. Das Ergebnis der Berechnung wird auf ganze Zahlen aufgerundet, da ein Funktionsablauf immer bis zum Ende des Verlaufs zu betrachten ist. Da es in einem Streckenbereich mehrere Gleise sowie Ein- oder Zweirichtungsbetrieb geben kann, wird das Ergebnis pro Zugfahrt mit der Betriebsdichte im Störungsbereich pro Std. alle Richtungen multipliziert. Das ergibt für das Beispiel in Abbildung 23 insgesamt 16 Funktionsabläufe pro Stunde bei einer Taktzeit von 15 Minuten bzw. 4 Funktionsabläufe pro Stunde bei einer Taktzeit von 30 Minuten im Störungsbereich mit Richtungsbetrieb auf einer zweigleisigen Strecke von 20 km Länge.

Die Logik der Berechnung kann wie folgt in Formel (12) zusammengefasst werden.

$$N_{FA} = D_{AR} * aufrunden\left(\frac{SL_{TB}}{V_B * T_{SR}} * 60\right) \quad (12)$$

- N_{FA} : Anzahl der Funktionsabläufe pro Std. im (Teil-)Bereich (Funktionsabläufe/Std.)
 D_{AR} : Betriebsdichte pro Std. im (Teil-)Bereich (Fahrten/Std. alle Richtungen)
 SL_{TB} : Streckenlänge im (Teil-)Bereich (km)
 V_B : Mittlere Beförderungsgeschwindigkeit im (Teil-)Bereich (km/h)
 T_{SR} : Mittlere Taktzeit im (Teil-)Bereich (min)

Die Anzahl des Funktionsablaufs im Störungsbereich eines Fdl kann auch durch den Einsatz des Zusatz-Fdl reduziert werden. Je nach den betriebstechnischen Möglichkeiten kann der Störungsbereich entweder nach Betriebsbereich oder nach Betriebsrichtung dem Zusatz-Fdl zugeteilt werden¹⁴. Eine Aufteilung nach der Betriebsrichtung wäre bei einer zweigleisigen Strecke sinnvoll, da die Anzahl der Funktionsabläufe bzw. die Auslastung des Fdl bei einer homogenen Betriebsdichte auf beiden Streckengleisen halbiert wird. Im Gegensatz dazu ist eine Aufteilung nach dem Betriebsbereich in der Regel nur sinnvoll, wenn ein Funktionsablauf einer Zugfahrt, z. B. die Zugfahrt $Z_{1(A \rightarrow C)}$ im 30-Minuten-Takt, im Fall einer Aufteilung nicht unnötig in zwei Funktionsabläufe aufteilt ist. Ansonsten wird die Zugfahrt nach der Aufteilung bei beiden Fdl jeweils einmal als Funktionsablauf gezählt. Das kann in diesem Fall dazu führen, dass sich das Versagenspotenzial der Fdl im Störungsbereich wegen der Doppelzählung der Funktionsabläufe trotz der Aufteilung des Betriebsbereichs erhöhen kann. Unten in Tabelle 16

¹⁴ Sofern das Stellwerk über die Funktion verfügt, ist es in dem heutigen System bereits möglich, den Kontrollbereich mit hoher Auslastung zu splitten und von dem anderen Fdl mit der niedrigen Arbeitsauslastung steuern zu lassen [140].

wird die Anzahl der Funktionsabläufe pro Std. nach der Transformation in eine Punkteskala mit 8 Klassen bzw. Auslastungsniveaus umgewandelt.

Tabelle 16: Punkteskala Faktor 3 – Intensität der Handlung

Anzahl Funktionsablauf pro Std.	Transformieren	Punkteskala	Rundungsfehler
f	$\log_{\sqrt{3}} f + 1$	Runden ($\log_{\sqrt{3}} f + 1$)	Δ (Punkteskala - Transformieren)
1	1,00	1	0,00
2	2,20	2	-0,20
3	2,91	3	0,09
4	3,41	3	-0,41
5	3,80	4	0,20
6	4,11	4	-0,11
7	4,38	4	-0,38
8	4,61	5	0,39
9	4,82	5	0,18
10	5,00	5	0,00
12	5,32	5	-0,32
15	5,70	6	0,30
20	6,20	6	-0,20
25	6,59	7	0,41
30	6,91	7	0,09
40	7,41	7	-0,41
50	7,80	8	0,20
60	8,11	8	-0,11

Aus der Formel (12) kann entnommen werden, dass eine höhere Anzahl von Funktionsabläufen nur bei einer großräumigen Störung ($SL_{SB} \uparrow$), bei einer sehr niedrigen Beförderungsgeschwindigkeit ($V_B \downarrow$) und / oder bei sehr kleinen Taktzeiten ($T_{SR} \downarrow$) vorkommt. Die Werte eines herkömmlichen Störungsszenarios haben einen eher kleinen Störungsbereich von z. B. 10 km, eine mittlere Beförderungsgeschwindigkeit von z. B. 40 km/h und einer mittleren Taktzeit von z. B. 15-20 Minuten. Daher liegt die Anzahl der Funktionsabläufe pro Std. im heutigen Störungsbetrieb meistens unter 25 bzw. Skala 7. Die obere Grenze wird jedoch subjektiv festgehalten, damit auch die zukünftigen Störungsszenarios mit evtl. innovativen Handlungsprozessen berücksichtigt werden können. Bei 60 Funktionsabläufen pro Std. bedeutet das zwar, dass der Fdl im Durchschnitt pro Minute einen Funktionsablauf starten bzw. beenden muss, jedoch könnte das auch durch innovative Handlungsprozesse, welche eine niedrige Basis-Versagenswahrscheinlichkeit haben, ausgeglichen werden.

Auslastungsniveau des Fdl

Nachdem die Punktestände aller drei Einflussfaktoren bestimmt wurden, kann das Auslastungsniveau des Fdl aus der Punktesumme der drei Einflussfaktoren und ggf. mit einer Gewichtung ausgerechnet werden. Die Punktesumme der drei Einflussfaktoren liegt dann zwischen 3 und 18. Bei einer Gewichtung steht die Überlegung dahinter, ob der Anstieg eines

Punkts der Dauer der Handlung genauso viel Einfluss haben sollte wie ein Punktanstieg des Umfangs der Handlung oder der Intensität der Handlung. Sofern es keine belastbare Kalibrierungsmöglichkeit gibt, kann die Gewichtung nur subjektiv von dem Anwender eingeschätzt werden. Im Anwendungsbeispiel in Kapitel 4 wird der Faktor Dauer der Handlung mit 0,5, der Faktor Umfang der Handlung mit 1,5 und der Faktor Intensität der Handlung mit 1,0 gewichtet. Das wird damit begründet, dass der Punktestand des Umfangs der Handlung auf die Anzahl der Handlungsabläufe zurückzuführen ist und der Handlungsablauf aus mehreren Teilhandlungsschritten besteht. Daher ist zu erwarten, dass der Einfluss eines zusätzlichen Handlungsablaufs größer als der Einfluss einer zusätzlichen Arbeitsstunde in der Störung sein sollte. Um die auslastungsbedingte Versagenswahrscheinlichkeit des Fdl pro Handlungsablauf aus der Basis-Versagenswahrscheinlichkeit ableiten zu können, wird die Basis-Versagenswahrscheinlichkeit zu der niedrigsten Punktesumme 3 zugeordnet. Mit dem Anstieg eines Punkts erhöht sich die Versagenswahrscheinlichkeit des Fdl auslastungsbedingt um ca. Faktor $\sqrt{3}$. In Tabelle 17 ist ein Beispiel einer solchen Zuordnungstabelle mit einer Basis-Versagenswahrscheinlichkeit von $1\text{E-}06$ Versagen/Handlungsablauf dargestellt.

Tabelle 17: Zuordnungsbeispiel einer auslastungsbedingten Versagenswahrscheinlichkeit des Fdl

Punktesumme Auslastung	Auslastungsbedingte Versagenswahrscheinlichkeit
Punkt	Versagen/Handlungsablauf
3	$1,00\text{E-}06$
4	$1,78\text{E-}06$
5	$3,16\text{E-}06$
6	$5,62\text{E-}06$
7	$1,00\text{E-}05$
8	$1,78\text{E-}05$
9	$3,16\text{E-}05$
10	$5,62\text{E-}05$
11	$1,00\text{E-}04$
12	$1,78\text{E-}04$
13	$3,16\text{E-}04$
14	$5,62\text{E-}04$
15	$1,00\text{E-}03$
16	$1,78\text{E-}03$
17	$3,16\text{E-}03$
18	$5,62\text{E-}03$

Bei der Ermittlung der auslastungsbedingten Versagenswahrscheinlichkeit ist zu beachten, dass der höchste Wert der auslastungsbedingten Versagenswahrscheinlichkeit nicht größer als 1 Versagen/Handlungsablauf sein darf, da 1 Versagen/Handlungsablauf die Bedeutung hat, dass der Fdl bei jedem einzelnen Handlungsablauf versagen würde. Das bedeutet auch: Wenn die Versagenswahrscheinlichkeit diese Grenze erreicht hat, wird sie nicht mehr mit dem Punktanstieg der Auslastung erhöht. Nachdem die auslastungsbedingte Versagenswahrscheinlichkeit des Fdl pro Handlungsablauf bestimmt wurde, kann das

Versagenspotenzial des Funktionsmodells (Akteur Fdl) in Kombination mit dem Funktionsmodell abgeleitet werden. Wie in Abbildung 24 dargestellt wird, ergibt sich das Versagenspotenzial des Funktionsmodells (Akteur Fdl) aus der Anzahl der Handlungsabläufe bzw. Betriebsfunktionen, die mit dem maßgeblichen Akteur Fdl identifiziert wurden, und der auslastungsbedingten Versagenswahrscheinlichkeit des Fdl pro Handlungsablauf. Da im Funktionsmodell alle Betriebsfunktionen unabhängig voneinander sind, kann die Anzahl der Handlungsabläufe mit Fdl direkt mit der auslastungsbedingten Versagenswahrscheinlichkeit pro Handlungsablauf multipliziert werden. Dadurch wird das Versagenspotenzial des Funktionsmodells (Akteur Fdl) pro Funktionsablauf bestimmt.

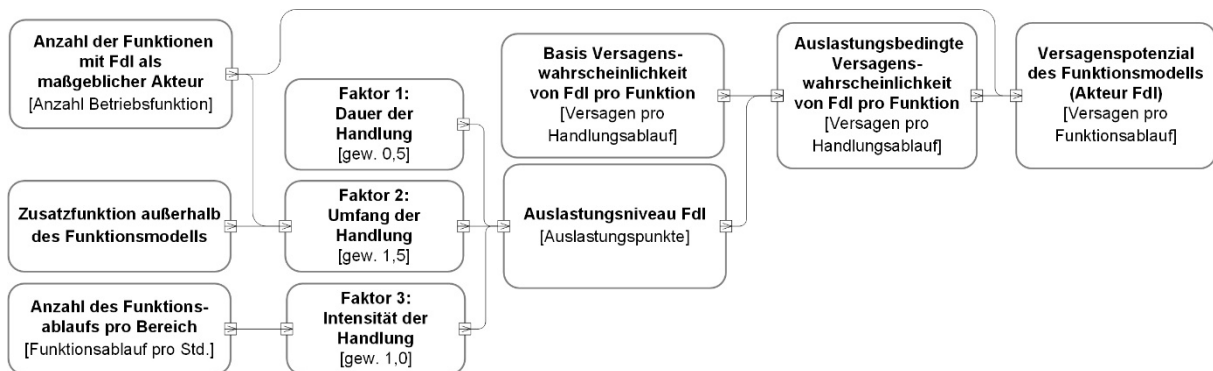


Abbildung 24: Konzept des Versagenspotenzials eines Funktionsmodells von Akteur Fdl

3.4.2.3.3 Versagenspotenzial Akteur Triebfahrzeugführer

Das Versagenspotenzial des Akteurs Triebfahrzeugführer beinhaltet die Versagenswahrscheinlichkeit aller Betriebsfunktionen, die den Tf als maßgeblichen Akteur haben. Wie die Abbildung 25 zeigt, wird die auslastungsbedingte Versagenswahrscheinlichkeit des Tf pro Betriebsfunktion aus einer Basis-Versagenswahrscheinlichkeit im Zusammenhang mit dem Auslastungsniveau des Tf abgeleitet. Das Auslastungsniveau des Tf wird anhand der Tätigkeitsänderung des Tf zwischen dem Regelbetrieb und dem Störungsbetrieb bestimmt.

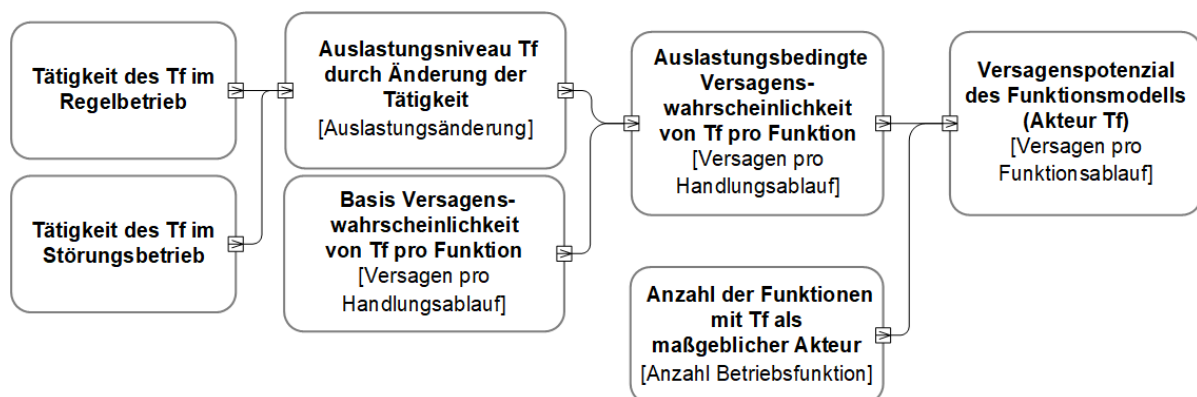


Abbildung 25: Konzept des Versagenspotenzials eines Funktionsmodells von Akteur Tf

Im Vergleich zur Ermittlung des Auslastungsniveaus des Fdl, das mithilfe genauer Angaben der Dauer, des Umfangs und der Intensität der Handlung bestimmt wird, wird bei der Bestimmung des Auslastungsniveaus des Tf lediglich die Änderung von dessen Tätigkeit im Regel- und Störungsbetrieb berücksichtigt. Das wird damit begründet, dass das Ziel der Bewertungssystematik eine schnelle Entscheidungsfindung eines Rückfallebenenkonzepts in der dynamischen Betriebslage ist. Es ist nicht vorgesehen, die genaue Auslastung der zahlreichen Tf im Störungsbereich im Einzelnen zu erfassen, was für den potenziellen Anwender in der Betriebszentrale heute auch schwer möglich wäre. Es werden daher die Einflussfaktoren „Fahrtätigkeit des Tf“ und „Fahrerlaubnis des Tf“ ausgewählt, die von dem Anwender in der Betriebszentrale im Zuge seiner fahrdienstlichen Handlungen sowie Verantwortlichkeit unmittelbar aus den verfügbaren Informationen entnommen werden können.

Bei dem Einflussfaktor Fahrtätigkeit des Tf wird berücksichtigt, wie die Fahrt von dem Tf realisiert wird. Nach dem Automatisierungsgrad des Fahrbetriebs, wie in [109] beschrieben, kann die Fahrtätigkeit des Tf in drei Kategorien aufgeteilt werden: „Manueller Fahrbetrieb ohne Zugbeeinflussung“, „Manueller Fahrbetrieb mit Zugbeeinflussung“ und „Halbautomatischer Fahrbetrieb“. Bei dem Einflussfaktor Fahrerlaubnis des Tf wird berücksichtigt, wie der Tf die maßgebliche Fahrerlaubnis erlangt hat. Es gibt im Grunde zwei Möglichkeiten: Entweder hat der Tf die maßgebliche Fahrerlaubnis fertigkeitstbasiert direkt aus der technischen Anzeige, wie z. B. von ortsfesten Signalen oder von der Führerraumanzeige abgelesen, oder er hat die maßgebliche Fahrerlaubnis regelbasiert nach einer aktiven Kommunikation mit dem Fdl als schriftlichen oder mündlichen Befehl erhalten. Im letzteren Fall muss der Tf die Anweisung im Befehl mit der örtlichen Gegebenheit vergleichen und dies während der Fahrt umsetzen. Durch die unterschiedliche Intensität in der Abwicklung der Fahrtätigkeit und der Fahrerlaubnis können unterschiedliche Auslastungen auch beim Tf entstehen. Analog zu dem Punktsystem des Auslastungsniveaus des Fdl wird hier zur Ermittlung des Auslastungsniveaus des Tf ebenfalls ein Punktsystem mit einer Bandbreite von ca. $\sqrt{3}$ angewendet. Das bedeutet, dass ein Anstieg eines Punktes im Auslastungsniveau eine Erhöhung der Versagenswahrscheinlichkeit des Tf um ca. Faktor $\sqrt{3}$ zur Folge hat. Im Grunde gilt folgende Regel: Je höher der Automatisierungsgrad einer Tätigkeit ist, desto kleiner ist der Auslastungspunkt des Tf.

Wie die Tabelle 18 zeigt, kann die Fahrt in einem technisch gesicherten Regelbetrieb entweder mit „Manuellem Fahrbetrieb mit Zugbeeinflussung“ oder „Halbautomatischem Fahrbetrieb“ durchgeführt werden. Im Fall eines halbautomatischen Fahrbetriebs bleibt dem Tf nach der Start-Bedienung lediglich die Aufgabe, die Strecke zu beobachten und auf Unvorhergesehenes zu reagieren. Im Gegensatz dazu hat der Tf im Fall eines manuellen Fahrbetriebs mit Zugbeeinflussung zwei zusätzliche Aufgaben, nämlich die „Geschwindigkeit beobachten“ und „Fahrzeug steuern“. Die dazugehörige Aufgabe „Signalisierung beobachten“ wird jedoch durch den Einflussfaktor „Fahrerlaubnis des Tf“ separat behandelt. Basierend auf der Anzahl der Aufgaben des Tf kann der Auslastungspunkt des Tf in der Fahrtätigkeit im Regelbetrieb durch eine logarithmische Transformation mit einer Basis von ca. $\sqrt{3}$ und eine

Punktverschiebung des Skalenanfangs von 0 auf 1 abgeleitet werden. Daraus ergibt sich im Fall eines manuellen Fahrbetriebs mit Zugbeeinflussung ein Auslastungspunkt von 3 und im Fall eines halbautomatischen Fahrbetriebs ein Auslastungspunkt von 1. Bei der Fahrerlaubnis wird angenommen, dass die maßgebliche Fahrerlaubnis im technisch gesicherten Regelbetrieb immer selbsttätig über technische Wege an den Tf übermittelt wird. Die Fahrerlaubnis via Befehl wird im Regelbetrieb daher nicht berücksichtigt. Im Vergleich zu der Fahrerlaubnis via Befehl hat die Fahrerlaubnis via Technik einen deutlich höheren Automatisierungsgrad und wird deshalb als Skalenanfang der Fahrerlaubnis mit Punkt 1 gesetzt. Zum Bestimmen der Auslastung des Tf im Regelbetrieb werden der Punktestand der Fahrtätigkeit (R_1) und der Punktestand der Fahrerlaubnis (R_2) summiert. Wie das Beispiel in Tabelle 18 zeigt, erhält der Tf bei einem halbautomatischen Fahrbetrieb ($R_1 = 1$ Pkt.) mit einer technisch vermittelten Fahrerlaubnis ($R_2 = 1$ Pkt.) eine Auslastungssumme (R_s) im Regelbetrieb von 2 Punkten.

Tabelle 18: Beispiel Tätigkeit des Tf und dessen Auslastung im Regelbetrieb

Fahrtätigkeit im Regelbetrieb	Auslastungspunkt (R_1)	Summe Auslastungspunkt → (R_s) im Regelbetrieb: $R_s = R_1 + R_2$
Manueller Fahrbetrieb mit Zugbeeinflussung	3	
Halbautomatischer Fahrbetrieb	1	
Maßgebliche Fahrerlaubnis im Regelbetrieb	Auslastungspunkt (R_2)	
Technik	1	

Im Fall eines Störungsbetriebs wird angenommen, dass die Fahrt nicht mehr halbautomatisch, sondern nur manuell mit oder ohne Zugbeeinflussung des Tf durchgeführt werden kann. Wie das Beispiel in Tabelle 19 zeigt, wird der Auslastungspunkt des Tf bei einem manuellen Fahrbetrieb ohne Zugbeeinflussung mit 5 Punkten eingeschätzt. Dieser Punktanstieg liegt aber nicht an der Anzahl der Aufgaben des Tf. Begründet wird das damit, dass der Tf beim manuellen Fahrbetrieb ohne Zugbeeinflussung ein höheres Konzentrationsniveau benötigt, um die Fahrt korrekt und sicher durchführen zu können. Dadurch wird auch ein höheres Auslastungsniveau des Tf eingeschätzt.

Tabelle 19: Beispiel Tätigkeit des Tf und dessen Auslastung im Störungsbetrieb

Fahrtätigkeit im Störungsbetrieb	Auslastungspunkt (S_1)	Summe Auslastungspunkt → (S_s) im Störungsbetrieb: $S_s = S_1 + S_2$
Manueller Fahrbetrieb ohne Zugbeeinflussung	5	
Manueller Fahrbetrieb mit Zugbeeinflussung	3	
Maßgebliche Fahrerlaubnis im Störungsbetrieb	Auslastungspunkt (S_2)	
Befehl	3	
Technik	1	

Bei der Fahrerlaubnis via Befehl wird ein Auslastungspunkt von 3 eingeschätzt, da der Tf hier im Vergleich zum direkten Ablesen der technischen Anzeige deutlich mehr Zeit- und Arbeitsaufwand benötigt, um die Fahrerlaubnis aus dem Befehl nachzuvollziehen und auch während der Fahrt vergleichend umzusetzen. Der Tf erhält dann z. B. bei einem manuellen

Fahrbetrieb ohne Zugbeeinflussung ($S_1 = 5$ Pkt.) mit der Fahrerlaubnis durch Befehl ($S_2 = 3$ Pkt.) eine Auslastungssumme (S_s) im Störungsbetrieb von 8 Punkten.

Zur Ermittlung der auslastungsbedingten Versagenswahrscheinlichkeit wird die Auslastungsänderung des Tf zwischen dem Regelbetrieb und dem Störungsbetrieb berücksichtigt. Als Vergleichsbasis der Auslastungsänderung wird das Auslastungsniveau des Tf im Regelbetrieb genommen. Falls das Auslastungsniveau im Störungsbetrieb (S_s) keinen Unterschied zu dem Auslastungsniveau im Regelbetrieb (R_s), d. h. keine Punktänderung ($A_s = 0$) aufweist, hat der Tf im Störungsbetrieb die gleiche Versagenswahrscheinlichkeit wie im Regelbetrieb. Es wird hier angenommen, dass die Versagenswahrscheinlichkeit des Tf im Regelbetrieb einer ausgewählten Basis-Versagenswahrscheinlichkeit entspricht, die durch den Anwender festzulegen ist, z. B. $1E-06$ Versagen/Handlungsablauf. Wie das Beispiel der Zuordnungstabelle in Tabelle 20 zeigt, wird am Tabellenanfang die Punktänderung von Null der ausgewählten Basis-Versagenswahrscheinlichkeit von $1E-06$ Versagen/Handlungsablauf zugeordnet. D. h.: Wenn der Tf seine Tätigkeit im Fall einer Störung von einem halbautomatischen Fahrbetrieb mit der technischen Fahrerlaubnis ($R_s = 2$ Pkt.) auf einen manuellen Fahrbetrieb mit der Fahrerlaubnis durch Befehl ($S_s = 8$ Pkt.) wechseln muss, dann hat der Auslastungspunkt des Tf einen Anstieg von 6 Punkten ($S_s - R_s = 6$ Pkt.). Dadurch erhöht sich die Versagenswahrscheinlichkeit des Tf auslastungsbedingt um ca. $(\sqrt{3})^6$ und liegt bei $3,16E-05$ Versagen/Handlungsablauf.

Tabelle 20: Zuordnungsbeispiel einer auslastungsbedingten Versagenswahrscheinlichkeit des Tf

Änderung des Auslastungspunkts (A_s) = Störungsbetrieb (S_s) – Regelbetrieb (R_s)	Auslastungsbedingte Versagenswahrscheinlichkeit des Tf
0	$1,00E-06$
2	$3,16E-06$
4	$1,00E-05$
6	$3,16E-05$

3.4.2.4 Strukturteil - Anzahl der Versagen

Der Strukturteil Anzahl der Versagen ist der Anlaufpunkt für die Zusammenführung von technischem und menschlichem Versagen eines betrachteten Funktionsmodells, bei dessen Anwendung in dem vorliegenden Betriebsszenario in Summe zu erwarten ist. Um die Zielvariable Betriebsrisiko pro betrachtetem Zeitabschnitt (Opfer/Zeitabschnitt) aus dem gesamten Versagenspotenzial eines Funktionsmodells und dem Schadensausmaß eines Versagens (Opfer/Versagen) ausrechnen zu können, muss das gesamte Versagenspotenzial eines Funktionsmodells die Einheit (Versagen/Zeitabschnitt) haben. Nach dem Kontext des Betriebsrisikos ist das gesamte Versagenspotenzial eines Funktionsmodells als die voraussichtliche Anzahl der Versagen unter der Anwendung des betrachteten Funktionsmodells im vorliegenden Betriebsszenario und betrachteten Zeitabschnitt aufzufassen. D. h.: Alle Versagen in einem betrachteten Zeitabschnitt, sowohl die Versagen eines technischen Systems als auch die Versagen der Menschen, müssen bei der Ermittlung des Betriebsrisikos als eine Ausgangsgröße zusammengefasst werden.

Das Versagenspotenzial eines Funktionsmodells wurde bisher im letzten Strukturteil getrennt nach dessen maßgeblichem Akteur abgeleitet. Eine direkte Zusammenführung des Versagenspotenzials der Technik und des Menschen zum gesamten Versagenspotenzial des Funktionsmodells ist nicht möglich. Wie die Abbildung 26 zeigt, hat erstens das Ergebnis des Versagenspotenzials eines Funktionsmodells aus dem Teil Technik die Einheit (Versagen/Betriebsstunde), während das Versagenspotenzial eines Funktionsmodells aus dem Teil Mensch die Einheit (Versagen/Funktionsablauf) hat. Deshalb ist vor der Zusammenführung noch eine Umrechnung notwendig. Zweitens betrachtet das bisherige Ergebnis aus dem letzten Kapitel 3.4.2.3 lediglich das Versagenspotenzial des Funktionsmodells in einer einzigen Betriebsstunde mit Technik oder in einem einzigen Funktionsablauf mit Menschen. Daher ist an dieser Stelle eine Hochrechnung des Versagenspotenzials nach dem vorliegenden Betriebsszenario erforderlich.

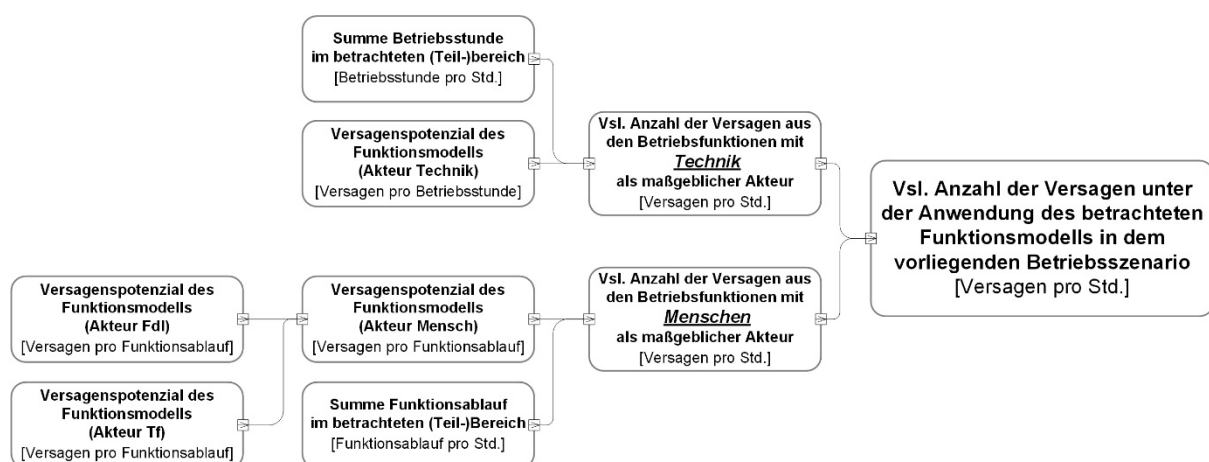


Abbildung 26: Zusammenführung von technischem und menschlichem Versagen im Funktionsmodell

Wie in Abbildung 26 dargestellt ist, erfolgt die Um- und Hochrechnung des Versagenspotenzials bei der Technik durch die Variable „Summe Betriebsstunden pro Std.“. Die Summe der Betriebsstunden bei der Technik wird näherungsweise durch die gesamten Reisezeiten aller Fahrten im betrachteten Bereich und Zeitabschnitt beschrieben. Die gesamten Reisezeiten im betrachteten Bereich pro Std. lassen sich, wie die Formel (13) darstellt, durch die Reisezeit einer Fahrt und die Betriebsdichte pro Std. im betrachteten Bereich näherungsweise bestimmen. Die Summe der Betriebsstunden hat dann die Einheit (Betriebsstunde/Std.). In Kombination mit dem Versagenspotenzial der Technik (Versagen/Betriebsstunde) lässt sich die vsl. Anzahl der vom maßgeblichen Akteur Technik resultierenden Versagen pro Std. in dem vorliegenden Betriebsszenario ausrechnen.

$$T_{SF} = D_{AR} * \frac{SL_{TB}}{V_B} \quad (13)$$

T_{SF}	Summe Reisezeiten aller Fahrten pro Std. im (Teil-)Bereich (Betriebsstunde/Std.)
D_{AR}	Betriebsdichte pro Std. im (Teil-)Bereich (Fahrten/Std. alle Richtungen)
SL_{TB}	Streckenlänge im (Teil-)Bereich (km)
V_B	Mittlere Beförderungsgeschwindigkeit im (Teil-)Bereich (km/h)

Bei der Um- und Hochrechnung des Versagenspotenzials des Menschen wird die Variable „Summe Funktionsabläufe pro Std.“ (Funktionsabläufe/Std.) herangezogen. Die Summe der Funktionsabläufe im betrachteten Bereich wurde bereits in Kapitel 3.4.2.3.2 ausführlich behandelt und kann anhand der Formel (12) eingeschätzt werden. Zusammen mit dem Versagenspotenzial des Menschen (Versagen/Funktionsablauf) kann die vsl. Anzahl der vom maßgeblichen Akteur Mensch resultierenden Versagen pro Std. im vorliegenden Betriebsszenario ausgerechnet werden.

Nach dem Vorgang der Umrechnung wird eine Zusammenführung des Versagenspotenzials der Technik und des Menschen ermöglicht. Das Versagenspotenzial eines Funktionsmodells, welches durch dessen Ausführung durch unterschiedliche Akteure in dem vorliegenden Betriebsszenario und dem betrachteten Zeitabschnitt zu erwarten ist, wird nach der Umrechnung und Zusammenführung als eine einzige Ausgangsgröße mit der Einheit (Versagen/Std.) zusammengefasst und lässt sich anschließend direkt bei der Ermittlung des Betriebsrisikos einsetzen.

3.4.2.5 Strukturteil - IT-Manipulationspotenzial

Nachdem die Anzahl der Versagen ermittelt wurde, folgt eine pauschale Betrachtung des Einflusses von IT-Security-Angriffen auf das Betriebsrisiko. In der bisher in Kapitel 3.4.2.4 ermittelten Anzahl der Versagen wurden lediglich solche Versagen betrachtet, deren Ursachen auf unbeabsichtigte und zufällige Ereignisse zurückzuführen sind. D. h., es wurden nur Safety-Ereignisse betrachtet. Allerdings können sowohl Safety-Ereignisse als auch Security-Ereignisse zum Versagen bzw. zum betrieblich gefährlichen Zustand im Bahnbetrieb führen, wie bereits in Kapitel 2.1 beschrieben. Zur Gewährleistung der Betriebsqualität müssen daher die Safety-Ereignisse sowie die Security-Ereignisse in ihrer Gesamtheit betrachtet werden. Um den Einfluss des IT-Security-Angriffs auf die Anzahl der Versagen im Bahnbetrieb berücksichtigen zu können, wird der Strukturteil bzw. die Variable IT-Manipulationspotenzial in die Bewertungssystematik eingeführt.

Die Variable IT-Manipulationspotenzial ist einheitslos und wirkt in der Berechnung als pauschaler Verstärkungsfaktor auf das Ergebnis der Anzahl der Versagen. Da bezüglich der Auswirkung des IT-Security-Angriffs bisher kein allgemein akzeptierter Faktorwert existiert, weder aus der Normung noch aus der Wissenschaft, sind die Faktorwerte im vorliegenden Abschnitt nur als Beispiel zu interpretieren. Wie in [112] beschrieben, liegt die Schwierigkeit der Wertschätzung bezüglich des IT-Security-Angriffs darin, dass aufgrund der sich dynamisch ändernden Bedrohungslage aus Statistiken der vergangenen Angriffe keine aussagekräftige Prognose abgeleitet werden kann. Der Fokus des vorliegenden Abschnitts liegt daher in der Vorstellung eines qualitativen Vorgehens zur Ermittlung des Verstärkungsfaktors. Die genaue Zuweisung der quantitativen Verstärkungsfaktorenwerte zu den qualitativen Ergebnissen des Vorgehens hat dann durch den Anwender im einzelnen Projekt oder in der Organisation zu erfolgen.

Im Grunde handelt es sich bei dem Konzept IT-Manipulationspotenzial um die Frage: „Wie wahrscheinlich ist es, dass das Bahnsystem im vorliegenden Betriebsszenario durch einen aktuellen IT-Security-Angriff kompromittiert wird, bei dessen Folge ein Versagen bzw. ein betrieblich gefährlicher Zustand im Bahnbetrieb zu erwarten ist?“ Nach [113–115] hängt die Wahrscheinlichkeit eines erfolgreichen Angriffs wesentlich von zwei Faktoren ab, nämlich von der Bedrohungslage der Systemumgebung und von dem IT-Schutzniveau des Systems.

3.4.2.5.1 Aktuelle Bedrohungslage der Systemumgebung

Bei der aktuellen Bedrohungslage der Systemumgebung wird die Wahrscheinlichkeit eines Angriffs eingeschätzt. Der Bedrohungslage der Systemumgebung kann z. B. durch die Aktivität des Angreifers, die aktuellen Vorfälle, den aktuellen Trend der Angriffsmethode oder das geopolitische Klima beeinflusst werden. Zur Einschätzung der Bedrohungslage der Systemumgebung wird das Vorgehen in IEC 62443-3-3 zugrunde gelegt. Nach IEC 62443-3-3 steht die Wahrscheinlichkeit eines Angriffs in einer Korrelation mit den Eigenschaften des Angreifers. Diese Eigenschaften sind die Methode, die Ressourcen, die Kenntnisse und die Motivation des Angreifers [112, 114]. Je nach dessen Eigenschaften lassen sich die Angreifer

nach IEC 62443-3-3 in drei Typen aufteilen. Im Rahmen dieser Bewertungssystematik wird die aktuelle Bedrohungslage der Systemumgebung mit einem bestimmten Angreifertyp korreliert. Befindet sich die Systemumgebung in einer bestimmten Stufe der Bedrohungslage, dann bedeutet das, dass der laufende Bahnbetrieb mit höchster Wahrscheinlichkeit unter dem Angriff eines bestimmten Angreifertyps stattfindet. Wie die Tabelle 21 darstellt, können die vier Stufen der Bedrohungslage der Systemumgebung wie folgt unterschieden werden:

- Bedrohungslage 0 (BL-0: Basis)

In der Bedrohungslage BL-0 (Basis) wird das System in der Regel nicht wirklich angegriffen. Es handelt sich im Grunde um die zufällige Fehlhandlung oder den vorhersehbaren Missbrauch durch das betriebliche Personal. Solche Fehlhandlungen oder Missbräuche werden üblicherweise bereits unter dem Aspekt des Safety-Ereignisses bei den sicherheitsrelevanten technischen Systemen im Bahnbereich berücksichtigt [112]. Die Bedrohungslage BL-0 wird daher als der normale Zustand der Systemumgebung angesehen.

- Bedrohungslage 1 (BL-1: Mittel)

In der Bedrohungslage BL-1 (Mittel) wird das System in der Regel von einer einfachen Methode angegriffen, die der Angreifer bereits mit einem geringen Ressourcenaufwand realisieren kann. Allerdings verfügt der Angreifer lediglich über allgemeine Kenntnisse über das von ihm angegriffene System. Außerdem ist die Motivation des Angreifers vergleichsweise gering. Er ist bei dem Angriff daher wenig hartnäckig.

- Bedrohungslage 2 (BL-2: Hoch)

In der Bedrohungslage BL-2 (Hoch) wird das System in der Regel von einer hochentwickelten Methode angegriffen. Der Angreifer verfügt zwar über die hochentwickelte Methode, hat aber nur moderate Ressourcen, um den Angriff durchzuführen. Allerdings besitzt der Angreifer systemspezifische Kenntnisse über das von ihm angegriffene System. Die Motivation des Angreifers ist vergleichsweise moderat und daher zeigt er auch mehr Entschlossenheit bei dem Angriff.

- Bedrohungslage 3 (BL-3: Extrem)

In der Bedrohungslage BL-3 (Extrem) wird das System in der Regel, wie in der Bedrohungslage BL-2, von einer hochentwickelten Methode angegriffen. Der Angreifer in der Bedrohungslage BL-3 besitzt, ebenfalls wie bei der Bedrohungslage BL-2, eine systemspezifische Kenntnis über das von ihm angegriffene System. Der entscheidende Unterschied liegt aber bei den verfügbaren Ressourcen und der Motivation des Angreifers in der Bedrohungslage BL-3. In der Bedrohungslage BL-3 verfügt der Angreifer über vergleichsweise erweiterte Ressourcen, um den Angriff umzusetzen. Auch die Motivation des Angreifers ist sehr hoch. Daher ist der Angreifer bei dem Angriff sehr zielstrebig und beharrlich.

Tabelle 21: Stufe der Bedrohungslage nach Angreifertyp in IEC 62443-3-3 [114]

		Eigenschaften des Angreifers			
Bedrohungslage (BL)		Methode	Ressourcen	Kenntnisse	Motivation
BL-0	Basis	(sollte bereits im Rahmen des Safety-Ereignisses behandelt)			
BL-1	Mittel	Einfach	Gering	Allgemein	Gering
BL-2	Hoch	Hochentwickelt	Moderate	Systemspezifisch	Moderate
BL-3	Extrem	Hochentwickelt	Erweitert	Systemspezifisch	Hoch

3.4.2.5.2 Aktuelles IT-Schutzniveau des Systems

Mit dem zweiten Faktor wird die Verwundbarkeit des Systems anhand des aktuellen IT-Schutzniveaus (SL-AS) dargestellt. Die Verwundbarkeit eines Systems, auch bekannt als die Vulnerabilität des Systems, ist nach [116] ein Maß für die anzunehmende Schadensanfälligkeit eines Systems in Bezug auf ein bestimmtes Ereignis. D. h.: In Bezug auf eine bestimmte Bedrohungslage ist ein System mit einem niedrigen IT-Schutzniveau im Grunde verwundbarer als ein System mit einem höheren IT-Schutzniveau. Das Konzept des aktuellen IT-Schutzniveaus (SL-AS) ist nicht zu verwechseln mit dem Konzept des „Erreichten Security-Level (SL-A)“ in der 62443-3-3. Das Konzept des erreichten Security-Level (SL-A) eines Systems beschreibt zwar auch das tatsächliche Schutzniveau eines bestimmten Systems im Betrieb, jedoch handelt es sich bei dem SL-A um ein normales Sicherheitsniveau des Systems nach Inbetriebnahme. Im Gegensatz dazu beschreibt das Konzept des aktuellen IT-Schutzniveaus (SL-AS) das aktuelle Sicherheitsniveau eines Systems, einschließlich des kompromittierten Systemzustands nach einem erfolgreichen IT-Security-Angriff. Das bedeutet: Wenn nach einem erfolgreichen Angriff z. B. Teile der Security-Schutzfunktion eines Systems kompromittiert wurden, befindet sich das System in einem bestimmten aktuellen IT-Schutzniveau (SL-AS), welches von den normalen Sicherheitsniveaus (SL-A) des Systems abweicht.

Das aktuelle IT-Schutzniveau kann als die Gegenseite der Bedrohungslage beschrieben werden. Je nach dessen Stärke kann das IT-Schutzniveau wie folgt in fünf Stufen unterschieden werden:

- **Aktuelles IT-Schutzniveau 0 (SL-AS 0: Kein)**

Ein System mit dem aktuellen IT-Schutzniveau 0 (SL-AS 0: Kein) bietet keinen oder nur einen sehr begrenzten Schutz gegen jede Art von Angreifern. Auch die Schutzfunktionen, die bei den sicherheitstechnischen Systemen unter dem Aspekt des Safety-Ereignisses eingesetzt wurden, können in diesem Systemzustand teils oder komplett aufgehoben oder kompromittiert werden.

- **Aktuelles IT-Schutzniveau 1 (SL-AS 1: Basis)**

Ein System mit dem aktuellen IT-Schutzniveau 1 (SL-AS 1: Basis) kann in der Regel höchstens der Bedrohungslage BL-0 (unbedeutend) entgegenwirken. Alle Schutzfunktionen, die üblicherweise bei den sicherheitstechnischen Systemen unter dem

Aspekt des Safety-Ereignisses berücksichtigt werden, sind in dem aktuellen Systemzustand noch funktionsfähig.

- **Aktuelles IT-Schutzniveau 2 (SL-AS 2: Mittel)**

Ein System mit dem aktuellen IT-Schutzniveau 2 (SL-AS 2: Mittel) hat mindestens die Schutzstärke des SL-AS 1 und bietet einen zusätzlichen Schutz gegen vorsätzliche Angriffe mit einer einfacheren Methode, die der Angreifer vermutlich bereits mit geringem Ressourcenaufwand, allgemeinen Kenntnissen und geringer Motivation realisieren kann. Dieses IT-Schutzniveau sollte höchstens bis zur Bedrohungslage BL-1(Mittel) noch einen ausreichenden Schutz gewährleisten können.

- **Aktuelles IT-Schutzniveau 3 (SL-AS 3: Stark)**

Ein System mit dem aktuellen IT-Schutzniveau 3 (SL-AS 3: Stark) hat mindestens die Schutzstärke des SL-AS 2 und bietet einen zusätzlichen Schutz gegen vorsätzliche Angriffe mit einer hochentwickelten Methode, die der Angreifer erst mit moderatem Ressourcenaufwand, systemspezifischen Kenntnissen und moderater Motivation realisieren kann. Dieses IT-Schutzniveau sollte dem System höchstens bis zur Bedrohungslage BL-2 (Hoch) noch einen ausreichenden Schutz gewährleisten können.

- **Aktuelles IT-Schutzniveau 4 (SL-AS 4: Extrem)**

Ein System mit dem aktuellen IT-Schutzniveau 4 (SL-AS 4: Extrem) hat mindestens die Schutzstärke des SL-AS 3 und bietet einen zusätzlichen Schutz gegen vorsätzliche Angriffe mit einer hochentwickelten Methode, die der Angreifer nur mit erweitertem Ressourcenaufwand, systemspezifischen Kenntnissen und hoher Motivation realisieren kann. Dieses IT-Schutzniveau sollte dem System höchstens bis zur Bedrohungslage BL-3 (Extrem) noch einen ausreichenden Schutz gewährleisten können.

Das aktuelle IT-Schutzniveau des Systems wird im Rahmen dieser Systematik nur allgemein nach 62443-3-3 zusammengefasst. Für eine umfassende Einschätzung des IT-Schutzniveaus eines Systems können z. B. das Framework for Improving Critical Infrastruktur Cybersecurity [117] oder das Cybersecurity Capability Maturity Model (C2M2) [118] herangezogen werden. Für eine tiefgründige Untersuchung des Schutzniveaus der einzelnen Funktionen können z. B. die Anforderungen von Common Criteria [119] angewendet werden. Egal welche Methode bei der Lageeinschätzung angewendet wird, entscheidend sind ein andauerndes System-Monitoring und eine Lageanalyse des Systems im laufenden Betrieb durch ein kompetentes IT-Security-Managementteam. Ohne einen nötigen Überblick und die Information über den Zustand des Systems kann die Lage mit keiner der Methoden korrekt eingeschätzt werden.

3.4.2.5.3 Manipulationsmatrix

Zum Bestimmen des aktuellen IT-Manipulationspotenzials im Bahnbetrieb aus den Faktoren „Bedrohungslage der Systemumgebung“ und „Aktuelles IT-Schutzniveau des Systems“ wird hier eine Manipulationsmatrix analog der Risikomatrix der IT-Sicherheitsbeurteilung in z. B.

IEC 62443-3-3 und IEC 27005 eingeführt. Durch die Manipulationsmatrix soll die Wahrscheinlichkeit einer erfolgreichen Manipulation durch die Beurteilung der aktuellen Bedrohungslage der Systemumgebung und des aktuellen IT-Schutzniveaus des Systems qualitativ bestimmt werden. Es ist zu beachten, dass es sich bei der vorliegenden Matrix nur um ein Beispiel handelt. Die genaue Zuweisung der qualitativen Skalenniveaus sowie der quantitativen Verstärkungswerte hat durch den Anwender der Systematik im einzelnen Projekt oder in der Organisation zu erfolgen.

Bei der Manipulationsmatrix werden auf der X-Achse die aktuelle Bedrohungslage der Systemumgebung (BL) und auf der Y-Achse das aktuelle IT-Schutzniveau des Systems dargestellt. Die Überschneidungen zwischen der Bedrohungslage und dem IT-Schutzniveau stellen das IT-Manipulationspotenzial dar. Wie die Tabelle 22 zeigt, ergibt die Überschneidung zwischen der höchsten Bedrohungslage (BL-3: Extrem) und dem niedrigsten IT-Schutzniveau (SL-AS 0: Kein) das höchste Manipulationspotenzial (Sehr hoch). Bei der Überschneidung zwischen einem IT-Schutzniveau und der dafür vorgesehenen Bedrohungslage ergibt sich das niedrigste Manipulationspotenzial (sehr gering). Da z. B. das IT-Schutzniveau SL-AS 3 (Stark) in der Regel einen ausreichenden Schutz gegen eine Manipulation in der Bedrohungslage BL-2 (Hoch) bieten kann, wird das Manipulationspotenzial bei dieser Kombination als „sehr gering“ eingeschätzt. Das Manipulationspotenzial unter einer bestimmten Bedrohungslage nimmt ab der Überschneidung mit dem vorgesehenen IT-Schutzniveau mit der Reduzierung des IT-Schutzniveaus zu. Hier werden fünf Skalenkategorien (Sehr hoch, Hoch, Moderat, Gering und Sehr gering) in der Beispielmatrix ausgewählt, um das Manipulationspotenzial zu differenzieren, wie die Tabelle 22 zeigt.

Tabelle 22: Beispiel für eine 4 x 5-Manipulationsmatrix mit fünf qualitativen Skalenkategorien

Aktuelles IT-Schutzniveau des Systems (SL-AS)		Aktuelle Bedrohungslage der Systemumgebung (BL)			
		BL-0 (Basis)	BL-1 (Mittel)	BL-2 (Hoch)	BL-3 (Extrem)
Kein	SL-AS 0	Gering	Moderate	Hoch	Sehr hoch
Basis	SL-AS 1	Sehr gering	Gering	Moderate	Hoch
Mittel	SL-AS 2	Sehr gering	Sehr gering	Gering	Moderate
Stark	SL-AS 3	Sehr gering	Sehr gering	Sehr gering	Gering
Extrem	SL-AS 4	Sehr gering	Sehr gering	Sehr gering	Sehr gering

Um den Einfluss des IT-Manipulationspotenzials als Verstärkungsfaktor auf die Anzahl der Versagen in der Berechnung des Betriebsrisikos berücksichtigen zu können, müssen die qualitativen Skalenkategorien den entsprechenden Faktorenwerten zugewiesen werden. Da bisher keine aussagekräftige Prognose aus Statistiken der vergangenen Angriffe abgeleitet werden kann, erfolgt die Zuweisung der Faktorenwerte im Rahmen dieser Arbeit nur beispielhaft und subjektiv. Es wird angenommen, dass die Anzahl der Versagen beim Anstieg einer Stufe des Manipulationspotenzials analog zu der Basis der logarithmischen Transformation des Versagenspotenzials um ca. Faktor $\sqrt{3}$ erhöht wird. Der Faktorenwert wird nach der Transformation konservativ auf ganze Zahlen aufgerundet. Wie die Tabelle 23 zeigt,

haben die Skalenkategorien des Manipulationspotenzials nach der Transformation einen Faktorenwert zwischen 1,0 bei Skala „Sehr gering“ und 10,0 bei Skala „Sehr hoch“. Bei der Skala „Sehr gering“ mit dem Faktorenwert 1,0 bedeutet das, dass die Anzahl der Versagen bzw. das Betriebsrisiko nicht durch das IT-Manipulationspotenzial beeinträchtigt wird. Im Vergleich dazu wird bei der Skala „Sehr hoch“ mit dem Faktorenwert von 10,0 vermutet, dass bei der Anzahl der Versagen bzw. des Betriebsrisikos aufgrund des Einflusses des IT-Manipulationspotenzials eine Erhöhung um Faktor 10 zu erwarten ist.

Tabelle 23: Beispiel für die Zuweisung von qualitativer Skala zu den Faktorenwerten

Potenzial der Manipulation		Transformieren	Faktorenwert
Skalenkategorie	Stufe X	$(\sqrt{3})^{(X-1)}$	Aufrunden $((\sqrt{3})^{(X-1)})$
Sehr gering	1	1,00	1,0
Gering	2	1,78	2,0
Moderate	3	3,16	4,0
Hoch	4	5,62	6,0
Sehr hoch	5	10,0	10,0

Nachdem die Skalenkategorie des Manipulationspotenzials dem entsprechenden Faktorenwert zugewiesen wurde, können die qualitativen Skalenkategorien in der Manipulationsmatrix in Tabelle 22 durch die Faktorenwerte ersetzt werden. Dadurch ergibt sich eine Manipulationsmatrix mit dem Faktorenwert als Ausgangsgröße an der Überschneidung der aktuellen Bedrohungslage und des aktuellen IT-Schutzniveaus, wie die Tabelle 24 zeigt.

Tabelle 24: Beispiel für eine Manipulationsmatrix mit der Zuordnung der Verstärkungsfaktoren

Aktuelles IT-Schutzniveau des Systems (SL-AS)		Aktuelle Bedrohungslage der Systemumgebung (BL)			
		BL-0 (Basis)	BL-1 (Mittel)	BL-2 (Hoch)	BL-3 (Extrem)
Kein	SL-AS 0	2,0	4,0	6,0	10,0
Basis	SL-AS 1	1,0	2,0	4,0	6,0
Mittel	SL-AS 2	1,0	1,0	2,0	4,0
Stark	SL-AS 3	1,0	1,0	1,0	2,0
Extrem	SL-AS 4	1,0	1,0	1,0	1,0

3.4.2.6 Strukturteil - Reduktionsfaktor

Durch den Strukturteil Reduktionsfaktor wird die Tatsache berücksichtigt, dass das Eintreten eines Versagens bzw. eines betrieblich gefährlichen Zustands im laufenden Betrieb nicht unbedingt einen Unfall zur Folge haben muss. Dies betrifft insbesondere bei solchen Versagen, in deren Konsequenz höchstwahrscheinlich mit einem Zusammenstoß von Eisenbahnfahrzeugen zu rechnen ist, zu. Das wird damit begründet, dass zwei Eisenbahnfahrzeuge bei einem Zusammenstoß entweder gegenläufig, seitlich oder in der gleichen Richtung miteinander kollidieren müssen. Falls sich jedoch nach dem Eintritt eines Versagens nur ein Eisenbahnfahrzeug im potenziellen Bereich der Kollision befindet, wird es auch keinen Zusammenstoß geben. Aus diesem Grund ist dieser Reduktionsfaktor lediglich bei der Unfallart Zusammenstoß anzuwenden. Bei anderen Unfallarten wie Entgleisung, Aufprall und Zusammenprall ist kein zweites Eisenbahnfahrzeug am Unfallgeschehen beteiligt. Daher wird der Reduktionsfaktor bei diesen Unfallarten nicht angewendet.

3.4.2.6.1 Konfrontationswahrscheinlichkeit

Die theoretische Grundlage des Reduktionsfaktors basiert auf der Warteschlangentheorie und es kann auf die Arbeit von Hinzen [77] verwiesen werden. In der Arbeit von Hinzen wird der Reduktionsfaktor als eine Konfrontationswahrscheinlichkeit von ungünstigen Umständen beschrieben. Die hier genannten ungünstigen Umstände beziehen sich auf den Zustand, dass sich zwei Eisenbahnfahrzeuge in zwei benachbarten Signalabschnitten befinden. D. h., bei der Konfrontationswahrscheinlichkeit von ungünstigen Umständen handelt es sich um die Wahrscheinlichkeit, dass zwei benachbarte Signalabschnitte gleichzeitig von zwei Eisenbahnfahrzeugen belegt sind.

Nach Hinzen lässt sich die Konfrontationswahrscheinlichkeit (W_K) in einem Betrachtungsbereich und Betrachtungszeitraum, hier z. B. ein Jahr, aus der Summe der Belegungszeiten aller Signalabschnitte im Jahr (B) geteilt durch die Summe der Betriebsstunden aller Signalabschnitte im Jahr (Z) ausrechnen, wie die Formel (14) zeigt.

$$W_k = \frac{B}{Z} \quad (14)$$

W_K : Konfrontationswahrscheinlichkeit

B : Summe der Belegungszeiten aller Signalabschnitte im Jahr (Betriebsstunde/Jahr)

Z : Summe der Betriebsstunden aller Signalabschnitte im Jahr (Betriebsstunde/Jahr)

Bei den Belegungszeiten (B) handelt es sich um die Summe der Belegungszeiten aller Verkehrsarten im Bereich und Zeitraum der Betrachtung. In der vorliegenden Berechnung werden drei Verkehrsarten betrachtet, nämlich SPFV, SPNV und SGV. Wie die Formel (15) zeigt, ergibt sich die Summe der Belegungszeiten einer bestimmten Verkehrsart j im Jahr (B_j) aus dem Produkt der Summe der Signalzugfahrten einer bestimmten Verkehrsart j im Jahr (N_{SZj}) und der mittleren Sperrzeit eines Signalabschnitts der bestimmten Verkehrsart j (T_{SPj}). Eine

Signalzugfahrt wird als eine Zugfahrt von einem Hauptsignal zu einem benachbarten Hauptsignal verstanden. Unter der Summe der Signalzugfahrten werden dann alle Zugfahrten von Hauptsignal zu Hauptsignal im Bereich der Betrachtung im Jahr berücksichtigt.

$$B_i = N_{SZ_j} * T_{SP_j} \quad (15)$$

- B_j : Summe der Belegungszeiten von Verkehrsart j im Jahr (Betriebsstunde/Jahr)
 N_{SZ_j} : Summe der Signalzugfahrten von Verkehrsart j im Jahr
 T_{SP_j} : Mittlere Sperrzeit eines Signalabschnitts von Verkehrsart j (h)
j : Die Verkehrsarten in der Betrachtung sind SPFV, SPNV und SGV

Die Summe der Signalzugfahrten einer bestimmten Verkehrsart j im Jahr (N_{SZ_j}) stellt sich als der Quotient aus der Summe der Verkehrsleistung einer bestimmten Verkehrsart j im Jahr (VL_j) und des mittleren Signalabstands im Bereich der Betrachtung (L_{SA}) dar, wie die Formel (16) zeigt.

$$N_{SZ_j} = \frac{VL_j}{L_{SA}} \quad (16)$$

- N_{SZ_j} : Summe der Signalzugfahrten von Verkehrsart j im Jahr
 VL_j : Summe der Verkehrsleistung von Verkehrsart j im Jahr (Trkm/Jahr)
 L_{SA} : Mittlerer Signalabstand (km)

Die mittlere Sperrzeit eines Signalabschnitts der Verkehrsart j (T_{SP_j}) ergibt sich dann aus der Summe der Fahrstraßenbildezeit (F_b), der Sichtzeit (S_z), der Annäherungsfahrzeit (L_V / V_{Bj}), der Fahrzeit im Signalabschnitt (L_{SA} / V_{Bj}), Räumfahrzeit ($L_D / V_{Bj} + L_{Zj} / V_{Bj}$) und der Fahrstraßenauflösezeit (F_a), wie die Formel (17) zeigt.

$$T_{SP_j} = F_b + S_z + \frac{L_V}{V_{Bj}} + \frac{L_{SA}}{V_{Bj}} + \frac{(L_D + L_{Zj})}{V_{Bj}} + F_a \quad (17)$$

- T_{SP_j} : Mittlere Sperrzeit eines Signalabschnitts der Verkehrsart j (h)
 F_b : Mittlere Fahrstraßenbildezeit (h)
 S_z : Sichtzeit (h)
 F_a : Mittlere Fahrstraßenauflösezeit (h)
 L_{Zj} : Mittlere Zuglänge der Verkehrsart j (km)
 V_{Bj} : Mittlere Beförderungsgeschwindigkeit der Verkehrsart j (km/h)
 L_V : Vorsignalabstand (km)
 L_D : Länge des Durchrutschwegs (km)
 L_{SA} : Mittlerer Signalabstand (km)
 V_{Bj} : Mittlere Beförderungsgeschwindigkeit der Verkehrsart j (km/h)
j : Die Verkehrsarten in der Betrachtung sind SPFV, SPNV und SGV

Bei der Summe der Betriebsstunden aller Signalabschnitte im Jahr (Z) werden die Betriebsstunden jedes einzelnen Signalabschnitts im Bereich der Betrachtung im Jahr betrachtet

und summiert. Die Summe der Betriebsstunden ergibt sich aus dem Produkt der Anzahl der Signalabschnitte im Bereich der Betrachtung (L_{HG} / L_{SA}) und der realen Stunden des Bahnbetriebs im Jahr (D_B). Bei den realen Betriebsstunden wird verstanden, dass die Betriebsstunden max. 24 Std. am Tag und max. 365 Tage im Jahr betragen. In der Summe betragen die realen Betriebsstunden im Jahr (D_B) max. 8760 Stunden. Die Anzahl der Signalabschnitte wird dann durch die Summe der Längen der Hauptgleise im Bereich der Betrachtung (L_{HG}) geteilt durch den mittleren Signalabstand (L_{SA}) näherungsweise eingeschätzt, wie die Formel (18) darstellt.

$$Z = \frac{L_{HG}}{L_{SA}} * D_B \quad (18)$$

Z : Summe der Betriebsstunden aller Signalabschnitten im Jahr (Betriebsstunde/Jahr)

L_{HG} : Summe der Längen der Hauptgleise

L_{SA} : Mittlerer Signalabstand (km)

D_B : Summe der realen Betriebsstunden im Jahr (Std./Jahr)

3.4.2.6.2 Beispielrechnung des Reduktionsfaktors

Im vorliegenden Abschnitt wird der Reduktionsfaktor bzw. die Konfrontationswahrscheinlichkeit am Beispiel des Schienenverkehrs auf dem öffentlichen Schienenverkehrsnetz in Deutschland im Bereich der DB-Netz AG berechnet.

Wie die Formel (18) zeigt, lässt sich die Summe der Betriebsstunden aller Signalabschnitte im Jahr (Z) aus der Länge der Hauptgleise, dem mittleren Signalabstand und der Summe der realen Betriebsstunden im Jahr ausrechnen. Wie bereits in Kapitel 3.3.2 beschrieben hat, kann die Gesamtlänge des Hauptgleises im öffentlichen Schienennetz in Deutschland anteilig auf ca. 61.300 km (= 67.400 km*91%) geschätzt werden. Um die Anzahl der Signalabschnitte näherungsweise einschätzen zu können, wird ein mittlerer Signalabstand von 3 km angenommen. Dieser mittlere Signalabstand von 3 km ergibt sich aus dem Mittelwert des Signalabstands von ausgewählten Streckenstandards P230, M230, P160 I, P160 II, M160, und G120, wie in [120] angegeben wurde. Die Summe der realen Betriebsstunden in Höhe von 20 Std./Tag wird aus dem Mittelwert der oberen und der unteren Grenze der Betriebsstunden aller Streckenstandards einschließlich P300, R120, R80 und G50 nach [95] abgeleitet. Mit einer Annahme von 365 Betriebstagen im Jahr ergibt sich eine Summe von 7300 Betriebsstunden im Jahr. Die Summe der Betriebsstunden aller Signalabschnitte im Jahr (Z) lässt sich anschließend, wie in Tabelle 25 gezeigt wird, anhand der vorgegebenen Formel ausrechnen.

Als erster Schritt zur Ableitung der Summe der Belegungszeiten aller Signalabschnitte im Jahr (B) muss die Summe der Signalzugfahrten nach Verkehrsart ausgerechnet werden. Die Summe der Signalzugfahrten einer Verkehrsart ist nach der Formel (16) der Quotient aus der Summe der Verkehrsleistung und dem mittleren Signalabstand. Nach dem Statistischen Bundesamt [93] wurde im Jahr 2017 auf dem öffentlichen Schienenverkehrsnetz in Deutschland eine Verkehrsleistung in Summe von 1.385 Mio. Trkm erbracht. Darunter sind 139 Mio. Trkm des

SPFV, 977 Mio. Trkm des SPNV und 269 Mio. Trkm des SGV. Mit einem Signalabstand von 3 km im Netzdurchschnitt lässt sich die Summe der Signalzugfahrten nach Verkehrsart ausrechnen, wie die Tabelle 25 zeigt.

Als nächster Schritt zur Ermittlung der Summe der Belegungszeiten aller Signalabschnitte im Jahr (B) ist die mittlere Sperrzeit eines Signalabschnitts nach Verkehrsart (T_{spi}) separat nach der Formel (17) abzuleiten. Je nach der Verkehrsart wird bei der Berechnung eine mittlere Beförderungsgeschwindigkeit von 140 km/h im SPFV, 70 km/h im SPNV und 50 km/h im SGV gemäß Anhang A angenommen. Neben der Beförderungsgeschwindigkeit ist auch die Zuglänge jeder Verkehrsart bei der Berechnung der Sperrzeiten zu unterscheiden. Nach Angabe der DB AG [121] haben die Züge im Fernverkehr, z. B. der ICE 1, eine Zuglänge von 358 m, der ICE 2 von 205 m, der ICE 3 von 200 m und der ICE 4 von 346 m. Da sich die Zuglängen des ICE 2 und ICE 3 jeweils auf eine kuppelbare Zuginheit bezieht, liegt die Zuglänge im Fernverkehr in der Regel zwischen 200 bis 400 m. Für den SPFV wird daher in der Berechnung eine mittlere Zuglänge von 300 m angenommen. Im SPNV wird die Zuglänge eines Musterzugs im SPNV-Ballungsraum nach [122] angenommen. Der Musterzug im SPNV fährt in Doppeltraktion, z. B. 2x Baureihe 422/432, und hat eine Zuglänge von 140 m. Beim Bestimmen von Zuglängen im SGV wird die Tatsache berücksichtigt, dass über 60 Prozent der auf dem öffentlichen Schienenverkehrsnetz verkehrenden Güterzüge nach [55] weniger als 600 m lang sind. Außerdem fahren die Güterzüge in Deutschland im Durchschnitt mit 25 bis 30 Güterwaggons. Bei einer Annahme von 15 bis 20 m Länge pro Güterwaggon ergibt sich eine Zuglänge einschließlich der Lok zwischen ca. 400 und 600 m. Daher wird in der Berechnung für den SGV eine mittlere Zuglänge von 500 m angenommen.

Für die übrigen Parameter, die bei der Berechnung nicht zwischen den Verkehrsarten unterschieden werden müssen, wird auf die Angabe von Hinzen [77] verwiesen. Nach Hinzen [77] ist eine Fahrstraßenbildezeit (F_b) von 0,2 min, eine Sichtzeit (S_z) von 0,2 min, ein Vorsignalabstand (L_v) von 1000 m, ein Durchrutschweg (L_D) von 200 m und eine Fahrstraßenauflösezeit (F_a) von 0,1 min anzunehmen. Mit den obigen Parametern lassen sich die Belegungszeiten aller Signalabschnitte im Jahr in Kombination mit der Summe der Signalzugfahrten für jede Verkehrsart ausrechnen.

Aus der Summe aller Belegungszeiten geteilt durch die Summe der Betriebsstunden aller Signalabschnitte ergibt sich nach Tabelle 25 eine mittlere Konfrontationswahrscheinlichkeit von 0,25¹⁵ auf dem öffentlichen Schienenverkehrsnetz in Deutschland. D. h., dass mit einer mittleren Wahrscheinlichkeit von 25% erwartet wird, dass zwei benachbarte Signalabschnitte auf dem öffentlichen Schienenverkehrsnetz in Deutschland gleichzeitig von zwei Eisenbahnfahrzeugen belegt werden.

¹⁵ Das tatsächliche Ergebnis (0,23) wird auf 0,05 aufgerundet.

Tabelle 25: Berechnung der Konfrontationswahrscheinlichkeit am Beispiel von Deutschland

(Nr.)	Parameter	Einheit	Wert		
(a)	Länge der Hauptgleise (2017) ¹	km	61300		
(b)	Mittlerer Signalabstand ²	km	3		
(c)	Anzahl Signalabschnitte = (a)/(b)	Signalabschnitte	20433		
(d)	Summe realer Betriebsstunden im Jahr =(d1)*(d2)	Std./Jahr	7300		
	(d1) Summe Tage im Jahr	Tage	365		
	(d2) Summe Stunden am Tag ³	Std.	20		
(e)	Summe Betriebsstunden aller Signalabschnitten = (c)*(d)	Betriebsstunde/Jahr	149.163.333		
Nr.	Parameter	Einheit	SPFV	SPNV	SGV
(f)	Verkehrsleistung im Jahr (2017) ⁴	Mio. Trkm/Jahr	139	977	269
(g)	Signalzugfahrt = (f)/(b)	Fahrt/Jahr	46.333.333	325.666.667	89.666.667
(h)	Mittlere Beförderungsgeschwindigkeit ⁵	km/Std.	140	70	50
(i)	Sperrzeit ⁶	Std.	4,05E-02	7,03E-02	1,02E-01
	(i) = (i1+i2)/60 + (i3/1000)/(h) + (b)/(h) + [(i4+i5)/1000]/(h) + (i6)/(h)				
	(i1) Fahrstraßenbildezeit	min	0,2		
	(i2) Sichtzeit	min	0,2		
	(i3) Vorsignalabstand	m	1000		
	(i4) Mittlere Zuglänge ⁷	m	300	140	500
	(i5) Durchrutschweg	m	200		
	(i6) Fahrstraßenauflösezeit	min	0,1		
(j)	Belegungszeit = (g)*(i)	Betriebsstunde	1,88E+06	2,29E+07	9,18E+06
(k)	Summe Belegungszeit = Σ(j)	Betriebsstd./Jahr	33.956.354		
	Konfrontationswahrscheinlichkeit⁸ = (k)/(e)		0,25		

1. Länge der Hauptgleise im öffentlichen Schienennetz wird anteilig geschätzt, siehe Kapitel 3.3.2

2. Mittelwert der Streckenstandard P230, M230, P160 I, P160 II, M160, und G120 nach [120]

3. Mittelwert der Obergrenze und Untergrenze der Betriebsstunden aller Streckenstandards nach [95]

4. aus Betriebsdaten des Schienenverkehrs 2017 des Statistischen Bundesamts [93]

5. siehe Anhang A

6. Variable i1 - i3 und i5 - i6 nach Hinzen [77]

7. SPFV, SPNV, SGV jeweils nach [121], [122] und [55] eingeschätzt

8. Ergebnis wird auf 0,05 aufgerundet

Wird die Konfrontationswahrscheinlichkeit wie in der vorliegenden Arbeit als Reduktionsfaktor des Unfallgeschehens angewendet, dann bedeutet das, dass im Netzdurchschnitt nur in 25% der Fälle eines Versagens bzw. eines betrieblich gefährlichen Zustands mit einem Beinahe-unfall oder Unfall als Folge zu rechnen ist. Allerdings muss beachtet werden, dass es sich bei diesem Wert von 25% lediglich um einen Netzdurchschnitt handelt. Das bedeutet, dass dieser durchschnittliche Wert nur auf ein Streckengleis mit der durchschnittlichen Betriebsdichte bzw. Streckenauslastung anzuwenden ist. Im Grunde ist zu erwarten, dass die Konfrontationswahrscheinlichkeit von zwei Eisenbahnfahrzeugen in benachbarten Abschnitten mit dem Anstieg der Betriebsdichte zunimmt und dadurch der Effekt der Reduktion des Unfallgeschehens geringer wird. Um den Reduktionsfaktor bei der Ermittlung des Betriebsrisikos entsprechend der aktuellen Betriebsdichte anpassen zu können, muss der Reduktionsfaktor im Netzdurchschnitt der durchschnittlichen Betriebsdichte im Netz

zugeordnet werden. Bei der Einschätzung der durchschnittlichen Betriebsdichte im Bereich der DB Netz AG werden die planerischen Streckenstandards der Richtlinie 413.0301 [95] der DB Netz AG zugrunde gelegt. Sowohl die Obergrenze als auch die Untergrenze der Betriebsdichte eines Streckengleises am Tag sind in der Richtlinie getrennt nach Streckenstandards vorgegeben. Neben der Angabe der Betriebsdichte am Tag wurden jeweils für die Ober- und Untergrenze der Betriebsdichte jedes Streckenstandards auch die Standard-Betriebsstunden jedes Streckenstandards als Tagesganglinie dargestellt. Dadurch lässt sich die mittlere Betriebsdichte eines Streckenstandards am Tag nach deren Ober- und Untergrenze der Betriebsdichte und deren Standard-Betriebsstunden separat ausrechnen, wie die Spalten „Mittlere Obergrenze“ und „Mittlere Untergrenze“ in Tabelle 26 zeigen. Die durchschnittliche Betriebsdichte eines Streckenstandards ergibt sich als Mittelwert der mittleren Obergrenze und der mittleren Untergrenze. Angesichts der unterschiedlichen Streckenlängen der jeweiligen Streckenstandards wird zur Ermittlung der durchschnittlichen Betriebsdichte im gesamten Netzbereich die durchschnittliche Betriebsdichte eines Streckenstandards mit dessen Gleislänge gewichtet. Daraus ergibt sich eine durchschnittliche planerische Betriebsdichte im Netzbereich der DB Netz AG von 3,5 Zügen/Std. je Richtung, wie die Tabelle 26 zeigt.

Tabelle 26: Mittlere planerische Streckenauslastung im Bereich der DB Netz AG nach [45, 95]

Streckenstandard	Streckenlänge ¹ (2017) in km	Anzahl Gleise	Planerische Streckenauslastung (Züge/Std. je Richtung)		
			Mittlere Obergrenze ²	Mittlere Untergrenze ³	Durchschnitt
P 300	1028	2	6,3	2,1	5
P 230	1158	2	5,7	2,1	4
M 230	968	2	6,3	2,5	5
P 160 I	1470	2	6,8	3,5	6
P 160 II	3246	2	3	2,1	3
M 160	5507	2	6,3	1,9	5
G 120	5073	2	4,2	1,8	4
R 120	7830	2	2,6	1,3	2
R 80	5987	1	1,6	0,9	2
G 50	919	1	1	-	1
Netzdurchschnitt ⁴					3,5

1. aus Infrastrukturzustands- und -entwicklungsbericht 2017 der DB Netz AG [45]

2. Mittlere Obergrenze ergibt sich aus der Obergrenze der Züge am Tag geteilt durch die Betriebsstunden am Tag

3. Mittlere Untergrenze ergibt sich aus der Untergrenze der Züge am Tag geteilt durch die Betriebsstunden am Tag

4. Streckenauslastung im Netzdurchschnitt wurde mit der Gleislänge des Streckenstandards im Jahr 2017 gewichtet

Um den Reduktionsfaktor entsprechend der Betriebsdichte anpassen zu können, wird die durchschnittliche Betriebsdichte von 3,5 Zügen/Std. je Richtung, aufgerundet auf 4 Züge/Std. je Richtung, als Vergleichsbasis zum durchschnittlichen Reduktionsfaktor von 0,25 zugeordnet, wie die Tabelle 27 zeigt. Durch eine logarithmische Transformation mit einer Basis von ca. $\sqrt[3]{3}$ wird die Betriebsdichte zwischen 1 und 40 Zügen/Std. je Richtung auf eine Punkteskala zwischen 1 und 7 transformiert. Es folgt eine Verschiebung der Punkteskala um minus 3 Punkte, damit der Punktestand der Vergleichsbasis auf dem Nullpunkt steht. Das bedeutet, dass bei

einer Betriebsdichte von 4 Zügen/Std. je Richtung keine Anpassung des Reduktionsfaktors notwendig ist. Ein Punktestand von minus 1 hat die Bedeutung, dass der Reduktionsfaktor um eine Stufe bzw. um den Faktor $\sqrt[3]{3}$ von 0,25 auf 0,14 reduziert wird. Das gleiche gilt auch bei einem Punktanstieg. Bei einem Punktestand von plus 1 bedeutet das, dass der Reduktionsfaktor um eine Stufe bzw. um den Faktor $\sqrt[3]{3}$ von 0,25 auf 0,44 erhöht wird. Es ist aber zu beachten, dass der Reduktionsfaktor einen Grenzwert von 1,0 hat. Sobald der Grenzwert bei einem Punktanstieg erreicht ist, bleibt der Reduktionsfaktor bei einem weiteren Punktanstieg unverändert. Das ist z. B. in Tabelle 27 bei dem Punktanstieg von 3 Punkten auf 4 Punkte zu sehen. Da der Reduktionsfaktor bei dem Punktestand 3 bereits den Grenzwert von 1,0 erreicht hat, ist der Reduktionsfaktor trotz eines weiteren Anstiegs auf Punktestand 4 weiterhin unverändert geblieben.

Tabelle 27: Beispiel einer Zuordnungstabelle von Betriebsdichte und Reduktionsfaktor

Züge pro Std. & Richtung	Transformieren & Runden	Verschieben	Reduktionsfaktor
z	$\text{Runden}(\log_{\sqrt[3]{3}} z + 1)$	$\text{Runden}(\log_{\sqrt[3]{3}} z + 1) - 3$	Quote
1	1	-2	0,08
2	2	-1	0,14
3	3	0	0,25
4	3	0	0,25
5	4	1	0,44
6	4	1	0,44
7	4	1	0,44
8	5	2	0,79
9	5	2	0,79
10	5	2	0,79
12	5	2	0,79
15	6	3	1,00
20	6	3	1,00
25	7	4	1,00
30	7	4	1,00
40	7	4	1,00

3.4.2.7 Strukturteil - Schadensausmaß

Nachdem das Versagenspotenzial eines Funktionsmodells in dem vorliegenden Betriebsszenario und dem betrachteten Zeitabschnitt unter der Betrachtung des IT-Manipulationspotenzials und des Reduktionsfaktors ermittelt wurde, bleibt das Einschätzen des maßgebenden Schadensausmaßes eines Versagens als letzter Schritt zum Bestimmen des Betriebsrisikos. Das maßgebende Schadensausmaß eines Versagens wird im Rahmen dieser Arbeit durch drei Variablen bestimmt, nämlich durch die Unfallart, die Unfallbeteiligten und die Unfallgeschwindigkeit, wie die Abbildung 27 zeigt.

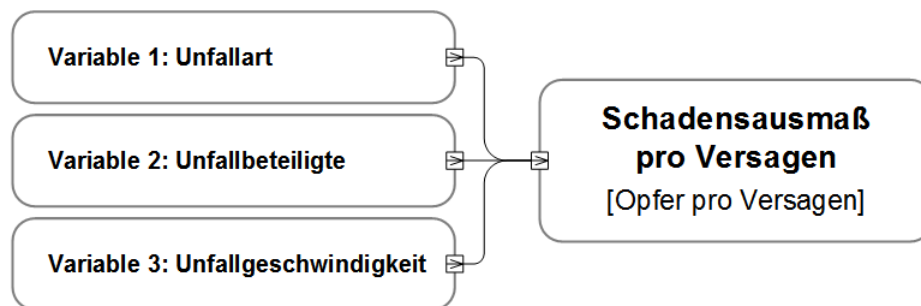


Abbildung 27: Variablen zum Bestimmen des Schadensausmaßes

Das gleiche Vorgehen zur Differenzierung von Unfallereignissen und deren Schadensausmaßen durch die genannten Variablen ist auch in der deutschen Normung VDE V 0831-103 (im Folgenden abgekürzt als VDE 103) zu finden. In der vorhandenen VDE 103 wird ein Unfallereignis aus dessen Unfallart, Unfallbeteiligten sowie dessen Unfallgeschwindigkeit zusammenhängend als eine generische Ereignisart beschrieben. Jede beschriebene Ereignisart wurde anhand dessen maßgebendem Schadensausmaß zu einer der sieben Unfallklassen, von A (kein Personenschaden) bis G (mehrere Todesfälle), zugeordnet. Die Klassifizierung des Schadensausmaßes erfolgt in VDE 103 semi-quantitativ durch Stichwörter wie „keine“, „ein“, „viele“ und „mehrere“ in der Kombination mit dem Verletzungsgrad wie „Leichtverletzte“, „Schwerverletzte“ und „Todesfall“. Die gesamten betrachteten generischen Ereignisarten und deren Unfallklassen sowie Schadensausmaße der VDE 103 befinden sich im Anhang B dieser Arbeit.

Zur Einschätzung des Schadensausmaßes in der Bewertungssystematik werden die vorhandenen Ereignisarten und die Klassifizierung des Schadensausmaßes aus der VDE 103 als Grundlage herangezogen. Die Klassen des Schadensausmaßes werden aber nach dem Anwendungskontext dieser Bewertungssystematik erweitert und angepasst. Auch die Darstellung der Zuordnung zwischen der Ereignisart und dem Schadensausmaß erhält für die Anwendung der Systematik eine neue Struktur, indem das Schadensausmaß nach der Unfallart, den Unfallbeteiligten und der Unfallgeschwindigkeit strukturiert und systematisch neu angeordnet wird.

3.4.2.7.1 Unfallart

Als erster Schritt zur Einschätzung des maßgebenden Schadensausmaßes eines Versagens ist die maßgebende Unfallart festzulegen. Je nach der Art des Funktionsversagens, wie in Kapitel 3.4.2.2 beschrieben, können unterschiedliche Unfallarten die Folge sein. Nach der VDE 103 sind mindestens vier Arten von Eisenbahnunfällen zu unterscheiden. Die vier Unfallarten sind nämlich der Aufprall, der Zusammenprall, die Entgleisung und der Zusammenstoß. Im Rahmen dieser Arbeit wird die Unfallart Frontalzusammenstoß, welcher in der Regel eine Unterkategorie der Unfallart Zusammenstoß ist, angesichts dessen erheblichen Schadenspotenzials im Vergleich zu einem üblichen Zusammenstoß in der gleichen Fahrrichtung separat aufgelistet. Dadurch werden fünf Unfallarten in der Systematik betrachtet. Die Unfallarten sind wie folgt voneinander zu unterscheiden:

- Aufprall

Beim Aufprall handelt es sich um das Auffahren eines Eisenbahnfahrzeugs auf ein Hindernis im Regellichtraum, z. B. Gleisabschluss, Gleissperre. Es wird davon ausgegangen, dass sich das Hindernis nur in einem Teil des Regellichtraums befindet, vorwiegend im unteren Bereich des Eisenbahnfahrzeugs, dieser aber nicht überwiegend oder vollständig belegt ist [40, 85, 123].

- Zusammenprall

Beim Zusammenprall handelt es sich um das Zusammentreffen eines Eisenbahnfahrzeugs mit einem Wegebenutzer auf einem Bahnübergang [85, 123].

- Entgleisung

Bei einer Entgleisung handelt es sich um ein Abgleiten oder Abheben eines Eisenbahnfahrzeugs von der Fahrbahn bei einer sich in Bewegung befindlichen Zugfahrt [85, 123].

- Zusammenstoß

Bei einem Zusammenstoß handelt es sich um das Auffahren eines Eisenbahnfahrzeugs auf ein anderes Eisenbahnfahrzeug in der gleichen Fahrrichtung, im Stillstand oder von der Seite als Flankenfahrt [85].

- Frontalzusammenstoß

Bei einem Frontalzusammenstoß handelt es sich um das Auffahren eines Eisenbahnfahrzeugs auf ein anderes fahrendes Eisenbahnfahrzeug in entgegengesetzter Fahrrichtung.

Das Störungsszenario, in dem mehrere Betriebsfunktionen betroffen sind, kann zwar auch mehrere Unfallarten, z. B. Entgleisung und Zusammenstoß, als Konsequenz haben. Zur Einschätzung des Betriebsrisikos wird jedoch für jedes Betriebsszenario in der Anwendung der Bewertungssystematik nur eine maßgebende Unfallart bestimmt. In diesem Fall ist die wahrscheinlichste Unfallart anstatt der schlimmsten Unfallart (Worst Case) als maßgebende

Unfallart anzunehmen. Da die Betriebsfunktionen in dem Funktionsmodell voneinander unabhängig sind, kann das Schadensausmaß in einer erweiterten Anwendung dieser Bewertungssystematik auch detailliert für jede Betriebsfunktionen getrennt bestimmt werden. Das voraussichtliche gesamte Schadensausmaß eines Betriebsszenarios lässt sich dann aus der Summe der einzelnen Betriebsfunktionen ausrechnen. Eine schnelle Einschätzung mit der Annahme der schlimmsten Unfallart ist zwar konservativ, deren Ergebnis liegt aber auf der sicheren Seite. Eine detaillierte Einschätzung kann auch nicht unbedingt sinnvoll sein, da z. B. ein Aufprall eine Entgleisung oder einen Zusammenstoß als Folge haben kann. Dadurch wäre die schnelle konservative Einschätzung zutreffender. Die Entscheidung, ob die wahrscheinlichste oder die schlimmste Unfallart maßgeblich ist sowie ob eine schnelle oder eine detaillierte Einschätzung des Betriebsrisikos anzuwenden ist, sollte aber von dem Anwender der Systematik anhand der aktuellen Betriebslage sowie der Bedrohungslage getroffen werden.

Auf der Liste in VDE 103 sind zwar noch weitere Ereignisarten, z. B. „Person wird von Schrankenbaum getroffen“, „Personenunfall an höhengleichem Bahnsteigzugang“ und „Personenunfall in einer Arbeitsstelle“, vorhanden. Diese Ereignisarten werden aber in der vorliegenden Bewertungssystematik nicht berücksichtigt, da es sich bei diesen Unfällen um Personen außerhalb des Zuges handelt, deren Schaden im Kontext des vorliegenden Betriebsrisikos nicht berücksichtigt wird. Außerdem ist zu beachten, dass das Funktionsmodell in dem Bewertungssystem die Betriebsfunktionen einer Zugfahrt abbildet. Daher fällt das Betriebsrisiko einer Rangierfahrt ebenfalls nicht in den Umfang der Betrachtung

3.4.2.7.2 Unfallbeteiligte

Nachdem die maßgebliche Unfallart festgelegt ist, kann als nächster Schritt der maßgebliche Unfallbeteiligte für das vorliegende Betriebsszenario bestimmt werden. Da bei dem Betriebsrisiko das Ausmaß des Personenschadens im Fokus steht, ist für die korrekte Ermittlung des Schadensausmaßes bzw. des Betriebsrisikos eine Differenzierung zwischen den Unfallbeteiligten im Güterverkehr und im Reiseverkehr notwendig. Außerdem wird berücksichtigt, dass außer bei den Unfallarten Zusammenstoß und Frontalzusammenstoß nur ein einziges Eisenbahnfahrzeug bei dem Unfallgeschehen benötigt wird. Dadurch unterscheidet sich der Unfallbeteiligte nicht nur von der Verkehrsart, sondern auch von der Anzahl des auslösenden Eisenbahnfahrzeugs.

Insgesamt werden hier vier Kategorien von Unfallbeteiligten definiert. Diese werden hier wie folgt beschrieben:

- **Kategorie 1: RZ**

Bei einem Unfall mit dem Unfallbeteiligten der Kategorie RZ ist immer nur ein Eisenbahnfahrzeug beteiligt, und zwar ein Reisezug. Es sind daher stets Fahrgäste im Zug zu erwarten.

- **Kategorie 2: GZ**

Bei einem Unfall mit dem Unfallbeteiligten der Kategorie GZ ist immer nur ein Eisenbahnfahrzeug beteiligt, und zwar ein Güterzug. Es befinden sich daher keine Fahrgäste im Zug.

- **Kategorie 3: GZ↔GZ**

Bei einem Unfall mit dem Unfallbeteiligten der Kategorie GZ↔GZ sind mindestens zwei Eisenbahnfahrzeuge beteiligt, und zwar nur Güterzüge. Es befinden sich daher keine Fahrgäste in den beiden Zügen.

- **Kategorie 4: GZ↔RZ / RZ↔RZ**

Bei einem Unfall mit dem Unfallbeteiligten der Kategorie GZ↔RZ / RZ↔RZ sind mindestens zwei Eisenbahnfahrzeuge beteiligt. Mindestens einer davon muss ein Reisezug sein. Der andere kann sowohl ein Reisezug als auch ein Güterzug sein. Es sind daher stets Fahrgäste in einem der beiden Züge zu erwarten.

Im Zusammenhang mit den Unfallarten lassen sich die Kategorien der Unfallbeteiligten zu den bestimmten Unfallarten zuordnen. Wie die Tabelle 28 zeigt, sind nicht alle Kombinationen der Unfallart und des Unfallbeteiligten nach der vorliegenden Definition möglich. Bei der Ermittlung des Schadensausmaßes werden daher nur die gültigen Kombinationen nach Tabelle 28 berücksichtigt.

Tabelle 28: Kombination von Unfallart und Unfallbeteiligten

Unfallbeteiligte	Unfallart				
	Aufprall	Zusammenprall	Entgleisung	Zusammenstoß	Frontal-zusammenstoß
RZ	Kombination gültig	Kombination gültig	Kombination gültig	-	-
GZ	Kombination gültig	Kombination gültig	Kombination gültig	-	-
GZ↔GZ	-	-	-	Kombination gültig	Kombination gültig
GZ↔RZ / RZ↔RZ	-	-	-	Kombination gültig	Kombination gültig

3.4.2.7.3 Unfallgeschwindigkeit

Die Unfallgeschwindigkeit bezieht sich nach VDE 103 nicht auf die mittlere Beförderungsgeschwindigkeit des Zuges, sondern auf die Geschwindigkeit zum Zeitpunkt des Unfalls. Bei der Annahme einer höheren Unfallgeschwindigkeit wandert das Ergebnis zwar zur sicheren Seite, kann das Leistungsniveau im Störungsbetrieb wegen des gebundenen höheren Betriebsrisikos aber deutlich einschränken. Zur Annahme einer niedrigen Unfallgeschwindigkeit muss auch eine zeitige Reaktion des Tf vorausgesetzt werden, was aber auch nicht immer möglich ist. Daher ist vom Anwender die Entscheidung zu treffen, ob die

maßgebliche Unfallgeschwindigkeit im Bereich der Betrachtung höher, gleich oder niedriger als die mittlere Beförderungsgeschwindigkeit sein sollte.

Zur Klassifizierung der Unfallgeschwindigkeit wurden in der VDE 103 bereits drei Klassen der Geschwindigkeit als Richtwerte vorgegeben. Diese sind:

- Niedrige Geschwindigkeit: bis einschließlich 40 km/h
- Mittlere Geschwindigkeit: über 40 km/h bis einschließlich 80 km/h
- Hohe Geschwindigkeit: über 80 km/h

Wie die Tabelle 29 zeigt, wird die Geschwindigkeitsklasse aus der VDE 103 im Rahmen dieser Bewertungssystematik um drei weitere Klassen auf insgesamt sechs Geschwindigkeitsklassen (Klasse 1 bis Klasse 6) erweitert. Die Geschwindigkeitsklasse 1 wird hier eingeführt, um einen Unfall ohne Personenschaden in einem extrem niedrigen Geschwindigkeitsbereich (nahe Null oder Schrittgeschwindigkeit) rechnerisch erfassen zu können. In diesem Fall wäre das Betriebsrisiko eines Unfalls ohne Personenschaden gleich Null. Ist diese Geschwindigkeitsklasse 1 nicht vorhanden, gehört ein Unfall im extrem niedrigen Geschwindigkeitsbereich nach VDE 103 zu der Geschwindigkeitsklasse „bis einschließlich 40 km/h“, in der nach deren Zuordnung stets mit einem Personenschaden zu rechnen ist. Das hat zur Folge, dass das Betriebsrisiko in diesem Fall unnötigerweise zu hoch eingeschätzt wird.

Tabelle 29: Klasse der Unfallgeschwindigkeit in der Bewertungssystematik

Geschwindigkeitsklasse	Unfallgeschwindigkeit (km/h)
1	$V \approx 0$
2	$V \leq 40$
3	$40 < V \leq 80$
4	$80 < V \leq 120$
5	$120 < V \leq 160$
6	$V > 160$

Im Gegensatz dazu werden die Geschwindigkeitsklassen 5 und 6 eingeführt, um das Betriebsrisiko im höheren Geschwindigkeitsbereich korrekt darstellen zu können. Die Geschwindigkeitsklasse 5 umfasst den Bereich über 120 km/h bis einschließlich 160 km/h und hat die gleiche Klassenbreite von 40 km/h wie die Klassen 2 bis 4. Bei einer Unfallgeschwindigkeit über 160 km/h gilt die Geschwindigkeitsklasse 6. Sind beide Geschwindigkeitsklassen nicht gegeben, werden alle Unfälle mit einer Geschwindigkeit von über 80 km/h nach VDE 103 zu der Geschwindigkeitsklasse „über 80 km/h“ zugeordnet. Nach der Zuordnung von VDE 103 ist z. B. bei einem Zusammenstoß mit einem Reisezug bei der Geschwindigkeitsklasse „über 80 km/h“ mit etwa 3 Todesfällen bzw. 3 Opfern nach Formel (1) zu rechnen. Sind beide Geschwindigkeitsklassen 5 und 6 nicht vorhanden, bedeutet das, dass sich die Anzahl der Opfer bei einem Unfall zwischen Unfallgeschwindigkeiten von z. B. 100 km/h, 140 km/h und 180 km/h nicht unterscheiden wird. Da das Schadensausmaß bei 3 Opfern pro Unfall nach VDE 103 konstant bleibt, wird das Betriebsrisiko in einem höheren Geschwindigkeitsbereich deutlich unterschätzt.

Mehrere nationale und internationale Eisenbahnunfälle haben gezeigt, dass es bei Eisenbahnunfällen in den Geschwindigkeitsklassen 5 und 6 bisher deutlich mehr als 3 Opfer geben kann, wie auch in Tabelle 30 steht. Z. B. hat es bei der Entgleisung eines Reisezugs mit 180 km/h (Geschwindigkeitsklasse 6) in Santiago des Compostela nach der Umrechnung 83 Opfer gegeben. Auch der Zusammenstoß zwischen einem Reisezug und einem Güterzug in Southall mit 130 km/h (Geschwindigkeitsklasse 5) hatte nach der Umrechnung 10 Opfer zur Folge. Bei dem Frontalzusammenstoß in Bad Aibling mit einer addierten Geschwindigkeit von 139 km/h gab es nach der Umrechnung 14 Opfer. Aus diesem Grund ist für die korrekte Einschätzung des Betriebsrisikos in dem höheren Geschwindigkeitsbereich die Einführung der Geschwindigkeitsklassen 5 und 6 sowie eine Anpassung deren entsprechender Opferzahlen unerlässlich.

Tabelle 30: Opferzahl der ausgewählten Unfällen in der Geschwindigkeitsklasse 5 und 6

Unfall	Eschede	Santiago de Compostela	Xinma	Southall	Ladbroke Grove	Bad Aibling
Jahr	1998	2013	2018	1997	1999	2016
Quelle	[124]	[125]	[126]	[127]	[128]	[129]
Unfallart	Entgleisung			Zusammenstoß	Fontalzusammenstoß	
Unfallbeteiligte	RZ	RZ	RZ	RZ-GZ	RZ-RZ	RZ-RZ
Unfallgeschwindigkeit	200 km/h	180 km/h	140 km/h	130 km/h	213 km/h (addiert)	139 km/h (addiert)
Geschwindigkeitsklasse	6	6	5	5	6	5
Reisenden im Zug	287	247	366	212	650	150
Getötete	101	80	18	7	31	12
Verletzte	88	140	187	139	523	89
Umgerechnete Opferzahl nach der Formel (2)	103	83	20	10	41	14

3.4.2.7.4 Anzahl der Opfer

Das Schadensausmaß eines Unfalls wurde in VDE 103 in sieben Unfallklasse A bis G aufgeteilt. Wie in Kapitel 3.3.2 beschrieben, lässt sich eine semi-quantitative Beschreibung der Unfallklassen in VDE 103 durch die Formel (1) auf eine Opferzahl zwischen 0 Opfer bei Unfallklasse A und 3 Opfer bei Unfallklasse G umrechnen. Um das Schadensausmaß in den höheren Geschwindigkeitsklassen 5 und 6 korrekt berücksichtigen zu können, werden die Unfallklassen im Rahmen der Arbeit um drei weitere Klassen H, I und J erweitert. Die Opferzahl der neuen Klasse wird entsprechend dem vorhandenen Klassensprung bei jedem Klasseanstieg um Faktor 3 erhöht. Dadurch haben die neuen Unfallklassen H, I und J jeweils die Opferzahl von 10, 30 und 100 Opfern pro Unfall, wie Tabelle 31 zeigt. Beim Festlegen der Unfallklasse anhand der Opferzahl ist zu beachten, dass jede Unfallklasse eine bestimmte Bandbreite hat. Z. B. hat die Opferzahl 10 aus der Unfallklasse H die Bedeutung, dass ein Unfall

in dieser Unfallklasse mindestens 10 Opfer haben muss, aber nicht mehr als 30 Opfer haben kann, welche der Mindestgrenze der Unfallklasse I entspricht.

Tabelle 31: Unfallklasse und deren Opferzahl in der Bewertungssystematik

Unfallklasse	Beschreibung in VDE 103	Ungerechnete Opferzahl	Bandbreite
A	Kein Personenschaden	0	0 \leq Anzahl der Opfer < 0,01
B	Ein Leichtverletzter	0,01	0,01 \leq Anzahl der Opfer < 0,03
C	Mehrere Leichtverletzte	0,03	0,03 \leq Anzahl der Opfer < 0,1
D	Ein Schwerverletzter oder viele Leichtverletzte	0,1	0,1 \leq Anzahl der Opfer < 0,3
E	Mehrere Schwerverletzte	0,3	0,3 \leq Anzahl der Opfer < 1
F	Ein Todesfall oder viele Schwerverletzte	1	1 \leq Anzahl der Opfer < 3
G	Mehrere Todesfälle	3	3 \leq Anzahl der Opfer < 10
H	(nicht vorhanden)	10	10 \leq Anzahl der Opfer < 30
I	(nicht vorhanden)	30	30 \leq Anzahl der Opfer < 100
J	(nicht vorhanden)	100	100 \leq Anzahl der Opfer

Um bei der Anwendung der Systematik die Anzahl der Opfer eines Unfalls direkt aus der Kombination aus Unfallvariablen (Unfallart, Unfallkombination und Unfallgeschwindigkeit) ableiten zu können, wird eine Zuordnungstabelle von den Unfallvariablen zu der Anzahl der Opfer vorausgesetzt. Bei der Zuordnung der Unfallvariablen zu der Opferzahl in den Geschwindigkeitsklassen 2 bis 4 wird die vorhandene Zuordnung aus der VDE 103 übernommen, wie dem Anhang B zu entnehmen ist. Anders als in der vorhandenen Zuordnung aus der VDE 103 wurden in der vorliegenden Arbeit folgende Anpassungen vorgenommen:

- Das Schadensausmaß der Geschwindigkeitsklasse 1 ($V \approx 0$) wird bei allen Unfallarten einheitlich mit der Unfallklasse A (Kein Personenschaden) angenommen.
- Die Unfallkombination „GZ“ und „GZ-GZ“ hat in allen Unfallarten, außer beim Frontalzusammenstoß, maximal die Geschwindigkeitsklasse 5 ($120 < V \leq 160$). Diese Geschwindigkeitsklasse 5 ist zwar höher als die in Deutschland nach der EBO [68] zulässige Geschwindigkeit der Güterzüge von 120 km/h. Das wird aber damit begründet, dass es sich bei dieser Geschwindigkeit um die Unfallgeschwindigkeit handelt, welche durchaus höher als die zulässige Betriebsgeschwindigkeit sein kann. Das Schadensausmaß der Geschwindigkeitsklasse 5 wird von der Unfallklasse der Geschwindigkeitsklasse 4 aus um eine Unfallklasse erhöht, bei der Unfallkombination „GZ“ und „GZ-GZ“ aber maximal nur bis zur Unfallklasse F (1 Opfer). Begründet wird dies damit, dass sich in jedem Güterzug häufig nur ein Tf befindet. Eine Unfallklasse G mit 3 Opfern ist für diese Unfallkombination daher nicht realistisch.

- Die Unfallart „Zusammenprall“ hat in allen Unfallkombinationen „RZ“ und „GZ“ maximal die Geschwindigkeitsklasse 5 ($120 < V \leq 160$), da in Deutschland auf Strecken mit einer Geschwindigkeit von über 160 km/h kein Bahnübergang erlaubt ist.
- Ausgehend von der Unfallklasse der Geschwindigkeitsklasse 4 wird das Schadensausmaß der Unfallkombinationen „RZ“ und „GZ↔RZ / RZ↔RZ“ der Geschwindigkeitsklasse 5 bei allen Unfallarten um eine Unfallklasse erhöht. Das Schadensausmaß der Geschwindigkeitsklasse 6 ist auf die gleiche Weise von der Unfallklasse der Geschwindigkeitsklasse 5 aus abzuleiten.
- Bei der Unfallgeschwindigkeit der Unfallart „Frontalzusammenstoß“ handelt es sich um die addierte Unfallgeschwindigkeit der beiden beteiligten Züge.

Die gesamten Zuordnungstabellen von Unfallart, Unfallkombination, Unfallgeschwindigkeit und Anzahl der Opfer befinden sich im Anhang C und sind nach der Unfallart getrennt aufgelistet.

3.4.3 Die Ergebnisse der Bewertung

3.4.3.1 Sicherheit des Bahnbetriebs

Die Ergebnisse der Betriebsrisiken der unterschiedlichen Rückfallebenenkonzepte lassen sich zwar direkt in absoluten Zahlenwerten vergleichen. Um jedoch das Maß des Risikoanstiegs anschaulich darstellen zu können, wird im Rahmen dieser Arbeit das Konzept Risikoindex verwendet. Der Risikoindex wird hier als das Verhältnis zwischen der Summe des Betriebsrisikos in einem bestimmten Zeitraum und dem Risikogrenzwert eines Kalenderjahrs im Bereich der Betrachtung definiert. Bei der Anwendung des Konzepts auf der Ebene des gesamten Netzes und in einem Zeitraum von Beginn des Kalenderjahrs bis zum Zeitpunkt t ergibt sich der Risikoindex (RI_{Nt}) zum Zeitpunkt t aus dem kumulierten Betriebsrisiko (KBR_{Nt}) und dem Risikogrenzwert des gesamten Netzes pro Kalenderjahr (RG_{NJ}), wie die Formel (19) zeigt.

$$RI_{Nt} = \frac{KBR_{Nt}}{RG_{NJ}} * 100\% \quad (19)$$

- RI_{Nt} : Risikoindex im gesamten Netz von Beginn des Kalenderjahrs bis zum Zeitpunkt t (%)
 KBR_{Nt} : Kumuliertes Betriebsrisiko im gesamten Netz von Beginn des Kalenderjahrs bis zum Zeitpunkt t (Opfer/Jahr)
 RG_{NJ} : Risikogrenzwert des gesamten Netzes pro Kalenderjahr (Opfer/Jahr)

Ähnlich wie bei dem Risikoindex im gesamten Netz (RI_{Nt}) lässt sich der Risikoindex in einem Fdl-Steuerbereich n im Zeitraum Δt durch das kumulierte Betriebsrisiko in dem betrachteten Fdl-Bereich im Zeitraum der Betrachtung ($KBR_{Bn,t \rightarrow t+\Delta t}$) und dem Risikogrenzwert dieses Fdl-Steuerbereichs pro Kalenderjahr (RG_{BJn}) bestimmen, wie die Formel (20) zeigt:

$$RI_{Bn,\Delta t} = \frac{KBR_{Bn,t \rightarrow t+\Delta t}}{RG_{BJn}} * 100\% = \frac{\sum_{i=1}^p BR_{Bn,i}}{RG_{BJn}} * 100\% \quad (20)$$

- $RI_{Bn,\Delta t}$: Der Risikoindex im betrachteten Fdl-Steuerbereich n vom Zeitpunkt t bis zum Zeitpunkt $t+\Delta t$ (%)
 $KBR_{Bn,t \rightarrow t+\Delta t}$: Kumuliertes Betriebsrisiko im betrachteten Fdl-Steuerbereich n vom Zeitpunkt t bis zum Zeitpunkt $t+\Delta t$ (Opfer/Jahr)
 RG_{BJn} : Der Risikogrenzwert eines Fdl-Steuerbereichs n pro Kalenderjahr (Opfer/Jahr)
 $BR_{Bn,i}$: Das Betriebsrisiko im betrachteten Fdl-Steuerbereich n in der Stunde i ($i = 1, \dots, p$) ab dem Zeitpunkt t bis zum Zeitpunkt $t+\Delta t$ (Opfer/Jahr)
 i : Die fortlaufende Stundenzahl vom Zeitpunkt t bis zum Zeitpunkt $t+\Delta t$
 p : Die letzte Stunde der Betrachtung vor dem Zeitpunkt $t+\Delta t$, die der Anzahl der Stunden vom Zeitpunkt t bis zum Zeitpunkt $t+\Delta t$ entspricht

Zur Kontrolle der Zulässigkeit eines Rückfallebenenkonzepts sind nach dem Konzept der Risiko-Budgetierung in Kapitel 3.3.3 zwei Bedingungen verbindlich festzuhalten. Die erste Bedingung ist der Risikogrenzwert des gesamten Netzes pro Kalenderjahr (RG_{NJ}). Die

Einhaltung des Risikogrenzwerts bedeutet, dass der Risikoindex den Grenzwert von 100% im gesamten Netz während eines Kalenderjahrs in der Regel nicht überschreiten darf. Die zweite Bedingung ist die durchschnittliche zulässige Anwendungsdauer des Rückfallebenenkonzepts in einem Fdl-Steuerbereich pro Kalenderjahr. Durch die Einschränkung der durchschnittlichen zulässigen Anwendungsdauer pro Kalenderjahr soll sichergestellt werden, dass kein Rückfallebenenkonzept mit einem übermäßig hohen stündlichen Betriebsrisiko zur Anwendung zugelassen wird. Um die Anwendungsdauer mit dieser Bedingung vergleichen zu können, ist im Rahmen jeder Bewertung die spezifische zulässige Anwendungsdauer eines Rückfallebenenkonzepts in einem Fdl-Steuerbereich pro Kalenderjahr¹⁶ zu ermitteln. Die spezifische zulässige Anwendungsdauer eines Rückfallebenenkonzepts pro Kalenderjahr in einem Fdl-Steuerbereich ergibt sich aus dem Quotienten der planmäßigen Risikoreserve pro Kalenderjahr und dem durchschnittlichen stündlichen Betriebsrisiko der Rückfallebenenkonzepte im Zeitraum der Betrachtung. Die planmäßige Risikoreserve pro Kalenderjahr in Form eines Risikoindex ist die Differenz zwischen dem Risikogrenzwert in einem Fdl-Bereich pro Kalenderjahr in Höhe von 100% und dem planmäßigen Risikoindex des Regelbetriebs (RI_{BRJn}) pro Kalenderjahr, welcher nach dem planmäßigen Jahresbetriebsprogramm zu erwarten ist. Wie später die Beispiele in Kapitel 4.4.2 zeigen werden, kann sich das stündliche Betriebsrisiko eines Rückfallebenenkonzepts wegen der Betrachtung der Arbeitsdauer von Menschen im Störungsbetrieb im Laufe eines betrachteten Zeitraums stündlich ändern. Außerdem können angesichts des Bedarfs in den unterschiedlichen Verkehrszeiten im Zeitraum der Betrachtung mehrere Rückfallebenenkonzepte kombinierend angewendet werden. Aus diesem Grund wird hier bei der Einschätzung der durchschnittliche Wert der stündlichen Betriebsrisiken im Zeitraum der Betrachtung anstatt des Betriebsrisikos einer bestimmten Stunde und eines bestimmten Rückfallebenenkonzepts verwendet. Das durchschnittliche stündliche Betriebsrisiko in Form eines Risikoindex ergibt sich dann aus dem Quotienten des Risikoindex im betrachteten Fdl-Steuerbereich im Zeitraum $t \rightarrow t + \Delta t$ ($RI_{Bn,\Delta t}$) und der Länge des Zeitraums (Δt), wie die Formel (21) zeigt.

$$AD_{n,k} = \frac{100\% - RI_{BRJn}}{\frac{RI_{Bn,\Delta t}}{\Delta t}} \quad (21)$$

$AD_{n,k}$:	Die spezifische Anwendungsdauer eines Rückfallebenenkonzepts k pro Kalenderjahr im betrachteten Fdl-Steuerbereich n (Std./Jahr)
RI_{BRJn} :	Planmäßiger Risikoindex des Regelbetriebs im betrachteten Fdl-Steuerbereich n pro Kalenderjahr (%)
$RI_{Bn,\Delta t}$:	Der Risikoindex im betrachteten Fdl-Steuerbereich n vom Zeitpunkt t bis zum Zeitpunkt $t+\Delta t$ (%)
Δt	Zeitraum zwischen dem Zeitpunkt t und dem Zeitpunkt $t+\Delta t$ (Std.)

¹⁶ Die Stundenschätzung erfolgt unter der Annahme eines konstanten Risikogrenzwerts pro Kalenderjahr in einem Fdl-Steuerbereich.

3.4.3.2 Leistungsniveau des Bahnbetriebs

Das Ergebnis Leistungsniveau des Bahnbetriebs wird im Rahmen dieser Bewertungssystematik durch die Beförderungsenergie dargestellt. Die Beförderungsenergie ist das Produkt aus der Beförderungsgeschwindigkeit des Zuges und der Betriebsdichte im Bereich der Betrachtung, wie in Kapitel 3.1.4 beschrieben. Bei der Ermittlung des Leistungsniveaus in einem Fdl-Steuerbereich ist zu beachten, dass sich der Bereich in der betrachteten Stunde i zum Teil im Regelbetrieb, zum Teil im Störungsbetrieb und zum Teil im Betriebsausfall befinden kann. Demnach ist das durchschnittliche Leistungsniveau in einem Fdl-Steuerbereich n in der Stunde i der Betrachtung ($LN_{Bn,i}$) anteilig nach der Gleislänge des jeweiligen Teilbereichs auszurechnen, wie die Formel (22) zeigt. Die Summe der Gleislängen der Teilbereiche im Störungsbetrieb (GL_{Bn}), im Regelbetrieb ($GL_{BRn,i}$) und im Betriebsausfall ($GL_{BA n,i}$) muss der Gleislänge im gesamten betrachteten Fdl-Steuerbereich entsprechen. Da das Leistungsniveau im Fall eines Betriebsausfalls stets Null beträgt, wird dieser Teilbereich in der Berechnung nicht berücksichtigt.

$$LN_{Bn,i} = LN_{BSn,i} * \frac{GL_{BSn,i}}{GL_{Bn}} + LN_{BRn,i} * \frac{GL_{BRn,i}}{GL_{Bn}} \quad (22)$$

$LN_{Bn,i}$: Durchschnittliches Leistungsniveau in dem gesamten Fdl-Steuerbereich n in der Stunde i

$LN_{BSn,i}$: Leistungsniveau im Teilbereich mit dem Störungsbetrieb in der Stunde i

$LN_{BRn,i}$: Leistungsniveau im Teilbereich mit dem Regelbetrieb in der Stunde i

GL_{Bn} : Gleislänge in dem gesamten Fdl-Steuerbereich n

$GL_{BSn,i}$: Gleislänge im Störungsbetrieb in dem Fdl-Steuerbereich n in der Stunde i

$GL_{BRn,i}$: Gleislänge im Regelbetrieb in dem Fdl-Steuerbereich n in der Stunde i

Um jedoch das Maß der Leistungsdifferenz anschaulich vergleichen zu können, wird das Ergebnis des Leistungsniveaus durch das Konzept Leistungsindex dargestellt. Der Leistungsindex wird in dieser Arbeit als Anteil des voraussichtlich erreichbaren Leistungsniveaus definiert, welches bei der Anwendung eines Betriebskonzepts oder Rückfallebenenkonzepts zu dem planmäßigen Leistungsniveau im Zeitraum und Bereich der Betrachtung zu erwarten ist. Bei der Betrachtung eines Fdl-Steuerbereichs und eines Zeitraums von einer Stunde lässt sich der Leistungsindex in einem Fdl-Steuerbereich n in der Stunde i ($LI_{Bn,i}$) anhand der Formel (23) bestimmen.

$$LI_{Bn,i} = \frac{LN_{Bn,i}}{LN_{RBn,i}} * 100 \quad (23)$$

$LI_{Bn,i}$: Leistungsindex in dem Fdl-Steuerbereich n in der Stunde i (%)

$LN_{Bn,i}$: Durchschnittliches Leistungsniveau in dem Fdl-Steuerbereich n in der Stunde i

$LN_{RBn,i}$: Leistungsniveau bei einem planmäßigen Regelbetrieb in dem gesamten Fdl-Steuerbereich n in der Stunde i

Bei der Kontrolle der Entwicklung des Leistungsniveaus in einem Fdl-Steuerbereich wird der Leistungsindex im Gegensatz zum Risikoindex nicht im Laufe der Zeit kumulativ summiert. Zur Bestimmung des Leistungsniveaus in einem Fdl-Steuerbereich über einen längeren Zeitraum wird als Ausgangsgröße stattdessen der Durchschnitt der Leistungsindexe von jeder Stunde im Zeitraum der Betrachtung genommen, wie die Formel (24) darstellt.

$$LI_{Bn,t \rightarrow t+\Delta t} = \frac{\sum_{i=1}^p LI_{Bn,i}}{p} \quad (24)$$

- $LI_{Bn,t \rightarrow t+\Delta t}$: Durchschnittlicher Leistungsindex in dem Fdl-Steuerbereich n im Zeitraum vom Zeitpunkt t bis zum Zeitpunkt t+ Δt (%)
- $LI_{Bn,i}$: Leistungsindex im Gesamtbereich der Betrachtung in der Stunde i (i = 1, ..., p) ab dem Zeitpunkt t bis zum Zeitpunkt t+ Δt (%)
- i: Die fortlaufende Stundenzahl vom Zeitpunkt t bis zum Zeitpunkt t+ Δt
- p: Die letzte Stunde der Betrachtung vor dem Zeitpunkt t+ Δt , die der Anzahl der Stunden vom Zeitpunkt t bis zum Zeitpunkt t+ Δt entspricht

Ist der durchschnittliche Leistungsindex jedes Fdl-Steuerbereichs im Zeitraum t \rightarrow t+ Δt bekannt, lässt sich der durchschnittliche Leistungsindex des gesamten Netzes ($LI_{Nt \rightarrow t+\Delta t}$) ebenfalls als Mittelwert des durchschnittlichen Leistungsindex jedes Fdl-Steuerbereichs im Netz darstellen, wie die Formel (25) darstellt.

$$LI_{Nt \rightarrow t+\Delta t} = \frac{\sum_{n=1}^q LI_{Bn,t \rightarrow t+\Delta t}}{q} \quad (25)$$

- $LI_{Nt \rightarrow t+\Delta t}$: Durchschnittlicher Leistungsindex in dem gesamten Netz im Zeitraum vom Zeitpunkt t bis zum Zeitpunkt t+ Δt (%)
- $LI_{Bn,t \rightarrow t+\Delta t}$: Durchschnittlicher Leistungsindex in dem Fdl-Steuerbereich n (n = 1, ..., q) im Zeitraum vom Zeitpunkt t bis zum Zeitpunkt t+ Δt (%)
- n: Die fortlaufende numerische Kennzeichnung des Fdl-Steuerbereichs in dem gesamten Netz
- q: Die höchste numerische Kennzeichnung des Fdl-Steuerbereichs, die der Anzahl der Fdl-Steuerbereiche in dem gesamten Netz entspricht

3.4.3.3 Verfügbarkeit des Bahnbetriebs

Bei dem Ergebnis Verfügbarkeit des Bahnbetriebs handelt es sich im Rahmen dieser Arbeit nach Kapitel 3.1.4 um die technische Verfügbarkeit. Im Kontext der technischen Verfügbarkeit wird der Bahnbetrieb im Bereich der Betrachtung als nicht verfügbar angesehen, solange eine Unregelmäßigkeit im System vorhanden ist und sich der Bahnbetrieb nicht komplett im technisch gesicherten automatisierten Regelbetrieb befinden. Der Verfügbarkeitsindex wird in dieser Arbeit als Verhältnis der Gleislänge im Regelbetrieb zur gesamten Gleislänge im Bereich und Zeitraum der Betrachtung definiert. Das bedeutet: Wenn sich die gesamte Gleislänge im Bereich und Zeitraum der Betrachtung im Störungsbetrieb und / oder im Betriebsausfall befindet, dann ist der Verfügbarkeitsindex in diesem Bereich und Zeitraum gleich Null. Bei der

Betrachtung eines Fdl-Steuerbereichs und eines Zeitraums von einer Stunde lässt sich der Verfügbarkeitsindex in einem Fdl-Steuerbereich n in der Stunde i ($VI_{Bn,i}$) anhand der Formel (26) bestimmen:

$$VI_{Bn,i} = \frac{GL_{BRn,i}}{GL_{Bn}} * 100 \quad (26)$$

- $VI_{Bn,i}$: Verfügbarkeitsindex in dem Fdl-Steuerbereich n in der Stunde i (%)
 $GL_{BRn,i}$: Gleislänge im Regelbetrieb in dem Fdl-Steuerbereich n in der Stunde i
 GL_{Bn} : Gleislänge in dem gesamten Fdl-Steuerbereich n

Ist die Verfügbarkeit des Bahnbetriebs über einen längeren Zeitraum $t \rightarrow t+\Delta t$ zu bestimmen, lässt sich der Verfügbarkeitsindex in einem Fdl-Steuerbereich n ($VI_{Bn,t \rightarrow t+\Delta t}$) in dem Zeitraum $t \rightarrow t+\Delta t$ durch den Mittelwert der Verfügbarkeitsindexe von jeder Stunde in diesem Zeitraum abbilden, wie die Formel (27) zeigt. Die Variable i in der Formel ist die fortlaufende Stundenzahl im Zeitraum $t \rightarrow t+\Delta t$, beginnend von 1 bis p. Die Größe der Variable p entspricht der Anzahl der Stunden im Zeitraum $t \rightarrow t+\Delta t$ und stellt die letzte Stunde der Betrachtung in dem betrachteten Zeitraum dar.

$$VI_{Bn,t \rightarrow t+\Delta t} = \frac{\sum_{i=1}^p VI_{Bn,i}}{p} \quad (27)$$

- $VI_{Bn,t \rightarrow t+\Delta t}$: Durchschnittlicher Verfügbarkeitsindex in dem Fdl-Steuerbereich n im Zeitraum vom Zeitpunkt t bis zum Zeitpunkt $t+\Delta t$ (%)
 $VI_{Bn,i}$: Verfügbarkeitsindex im Gesamtbereich der Betrachtung in der Stunde i ($i = 1, \dots, p$) ab dem Zeitpunkt t bis zum Zeitpunkt $t+\Delta t$ (%)
i: Die fortlaufende Stundenzahl vom Zeitpunkt t bis zum Zeitpunkt $t+\Delta t$
p: Die letzte Stunde der Betrachtung vor dem Zeitpunkt $t+\Delta t$, die der Anzahl der Stunden vom Zeitpunkt t bis zum Zeitpunkt $t+\Delta t$ entspricht

Letztendlich lässt sich die Verfügbarkeit des Bahnbetriebs in dem gesamten Netz während des Zeitraums $t \rightarrow t+\Delta t$ ($VI_{Nt \rightarrow t+\Delta t}$) durch den Mittelwert der durchschnittlichen Verfügbarkeitsindexe jedes Fdl-Steuerbereichs im Netz ($VI_{Bn,t \rightarrow t+\Delta t}$) darstellen, wie die Formel (28) zeigt.

$$VI_{Nt \rightarrow t+\Delta t} = \frac{\sum_{n=1}^q VI_{Bn,t \rightarrow t+\Delta t}}{q} \quad (28)$$

- $VI_{Nt \rightarrow t+\Delta t}$: Durchschnittlicher Verfügbarkeitsindex in dem gesamten Netz im Zeitraum vom Zeitpunkt t bis zum Zeitpunkt $t+\Delta t$ (%)
 $VI_{Bn,t \rightarrow t+\Delta t}$: Durchschnittlicher Verfügbarkeitsindex in dem Fdl-Steuerbereich n ($n = 1, \dots, q$) im Zeitraum vom Zeitpunkt t bis zum Zeitpunkt $t+\Delta t$ (%)
n: Die fortlaufende numerische Kennzeichnung des Fdl-Steuerbereichs in dem gesamten Netz
q: Die höchste numerische Kennzeichnung des Fdl-Steuerbereichs, die der Anzahl der Fdl-Steuerbereiche im gesamten Netz entspricht

Die Variable n in der Formel ist die fortlaufende numerische Kennzeichnung für den Fdl-Steuerbereich in dem gesamten Netz, beginnend von 1 bis q . Die Kennzeichnung q entspricht der Anzahl der Fdl-Steuerbereiche im gesamten Netz und ist die höchste numerische Kennzeichnung der Variable n .

4 Die Bewertungssystematik in der Anwendung

Nachdem die Bewertungssystematik in Kapitel 3 ausführlich behandelt wurde, wird die Anwendung der Bewertungssystematik in diesem Kapitel beispielhaft vorgeführt. Aufgrund der fehlenden Daten der genauen Fehlerwahrscheinlichkeit sowie der Ausfallrate soll die folgende Berechnung nur beispielhaft zeigen, wie der Ansatz anzuwenden ist. Der Ablauf der Bewertung kann in vier Phasen eingeteilt werden, wie die Abbildung 28 zeigt. Dazu gehören: die Grundparameter festlegen, das Störungsszenario bestimmen, die Qualität der Konzeptvariante ermitteln und zuletzt das Rückfallebenenkonzept gestalten.

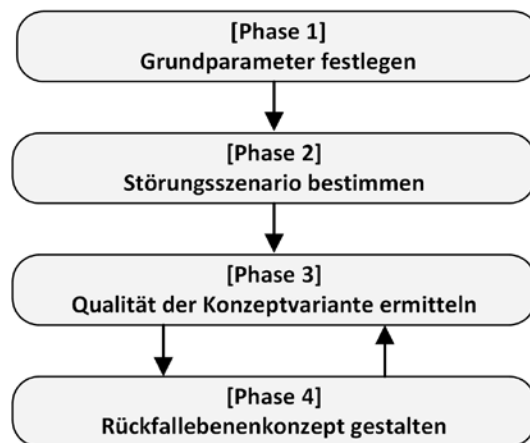


Abbildung 28: Ablauf der Bewertung

Vor Beginn der Bewertung werden die Grundparameter z. B. die Größe des betrachteten Fdl-Steuerbereichs in der Phase 1 festgelegt. Anschließend ist das Störungsszenario in der Phase 2 in dem betrachteten Fdl-Steuerbereich durch die Parameter zu erfassen. Die relevanten Parameter wie die Größe des betrieblichen Störungsbereichs, die betroffenen Betriebsfunktionen sowie das aktuelle IT-Manipulationspotenzial usw. wird in dieser Phase bestimmt. In der Phase 3 werden die Qualitäten der Varianten vom Rückfallebenenkonzept in dem betrachteten Fdl-Steuerbereich durch die Bewertungssystematik ermittelt. In der anschließenden Phase 4 werden die Rückfallebenenkonzepte unter der Berücksichtigung des Risikogrenzwertes strategisch gestaltet und beurteilt.

Da die Grundstruktur der Bewertungssystematik und deren Parameter zwecks einer Anwendung in dem Bereich eines Fdl-Steuerbereichs konstruiert und kalibriert wurden, wird die Vorführung der Bewertungssystematik in dem vorliegenden Kapitel lediglich beispielhaft anhand ihrer Anwendung in einem Fdl-Steuerbereich demonstriert. Die erweiterte Anwendung der Bewertungssystematik auf der Ebene des gesamten Netzes sowie die proaktive Steuerung vom Betriebsrisiko innerhalb eines Zeitraums und Netzes sind in den folgenden Beispielen nicht enthalten.

4.1 Phase 1: Die Grundparameter festlegen

Vor dem Beginn der Bewertung sind zunächst die Grundparameter festzulegen. Durch die Grundparameter werden z. B. die Größe des zu betrachteten Fdl-Steuerbereichs sowie dessen Betriebsparameter im planmäßigen Regelbetrieb erfasst. Die Grundparameter dienen zudem als Vergleichsbasis für die zu bewerteten Varianten des Rückfallebenenkonzepts.

In dem vorliegenden Beispiel befindet sich der betrachtete Fdl-Steuerbereich auf einer zweigleisigen Strecke. Die Streckelänge in dem betrachteten Fdl-Steuerbereich beträgt 40 km. Das entspricht einer Gleislänge von 80 km im Bereich der Betrachtung. Die Beispielstrecke entspricht dem Streckenstandard M160 der DB Netz AG und hat eine maximal zulässige Streckengeschwindigkeit von 160 km/h. In dem betrachteten Fdl-Steuerbereich befindet sich alle 20 km eine Zugmeldestelle (Zmst), in der die Reihenfolge der Züge auf der freien Strecke geregelt werden kann. Dieser Abstand von 20 km zwischen den Zmst wird gemäß der Untergrenze des Abstands zwischen den Überholungsbahnhöfen vom Streckenstandard M 160 ausgewählt [95]. Wie die Abbildung 29 zeigt, umfasst der betrachtete Fdl-Steuerbereich die Zmst A, die Zmst B sowie deren anschließenden freien Strecken. Die Zmst C gehört somit zum Steuerbereich des Nachbar-Fdl. Auf der Strecke wird ein Ks-Signalsystem eingebaut. Alle Signale, auch Signale auf der freien Strecke, haben eine Vor- und Hauptsignalfunktion. Der kleinste behinderungsfreie Zugfolgeabstand umfasst zwei Signalabschnitte und hat einen mittleren Abstand von 3 km. Sicherungstechnisch sind die Strecken mit der punktförmigen Zugbeeinflussung (PZB) ausgerüstet. Alle Züge fahren im Regelbetrieb unter der PZB-Überwachung.

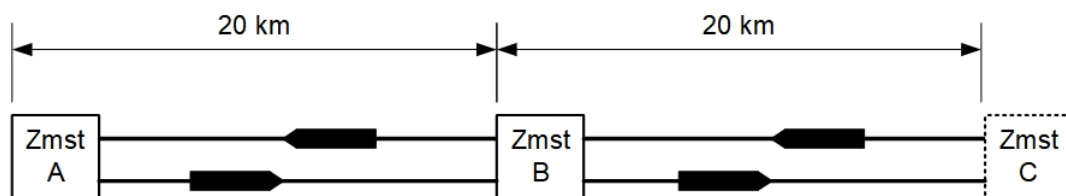


Abbildung 29: Schematische Darstellung des Gesamtbereichs der Betrachtung

Während des planmäßigen Regelbetriebs werden die Fahrten auf dem Streckengleis mit der Betriebsweise Einrichtungsbetrieb durchgeführt. Die durchschnittliche Betriebsdichte pro Streckengleis beträgt 5 Züge/Std. & Richtung für den Streckenstandard M 160, wie die Tabelle 26 zeigt. In Summe ergibt sich eine durchschnittliche Betriebsdichte von 10 Zügen/Std. alle Richtungen in dem betrachteten Fdl-Steuerbereich. Es fahren die Züge von SPFV, SPNV und SGV auf den Strecken. Die mittlere Beförderungsgeschwindigkeit beträgt in dem betrachteten Fdl-Steuerbereich 100 km/h. Der Fahrplan der Strecke hat eine inhomogene Struktur. Das bedeutet, dass die Reise- und Güterzüge wechselnd auf der Strecke gefahren werden. Eine Verkettung der artgleichen Züge ist im Fahrplan nicht gegeben.

Alle Betriebsfunktionen in dem Funktionsmodell haben im Regelbetrieb das technische System als maßgeblichen Akteur. Der Fdl hat während des Regelbetriebs nur eine überwachende

Funktion. Die Zugfahrt wird zwar manuell von dem Tf gesteuert, deren Durchführung wird aber von der Zugbeeinflussung überwacht und geschützt. Die maßgebliche Fahrerlaubnis erhält der Tf über Technik (Ortsfestes Signal). Eine Übersicht der wesentlichen Grundparametern des vorliegenden Beispielszenarios befindet sich in Tabelle 32.

Tabelle 32: Grundparameter des Beispielszenarios

Parameter	Wert	Einheit
§ Gesamtbereich der Betrachtung		
- Streckenlänge im Gesamtbereich	40	km
- Anzahl der Streckengleise	2	Streckengleis
- Gleislänge im Gesamtbereich	80	km
- Streckenstandard (optional)	M 160	
- Entfernung zwischen den Zugmeldestellen	20	km
§ Planmäßige Betriebsparameter im Regelbetrieb		
- Betriebsweise	Einrichtungsbetrieb	-
- Betriebsdichte pro Streckengleis	5	Züge/Std. & Richtung
- Betriebsdichte aller Streckengleise	10	Züge/Std. alle Richtungen
- Mittlere Beförderungsgeschwindigkeit	100	km/h
- Maßgebliche Verkehrsart	GZ-RZ / RZ-RZ	-
§ Funktionsmodell		
- [F1] Fahrweg sichern	(TS) Technisches System	-
- [F2] Abstandhaltung sichern	(TS) Technisches System	-
- [F3] Bahnübergang sichern	(TS) Technisches System	-
- [F4] Fahrerlaubnis bereitstellen	(TS) Technisches System	-
- [F5] Geschwindigkeit signalisieren	(TS) Technisches System	-
- [F6] Brems- & Antriebskräfte bereitstellen	(TS) Technisches System	-
- [F7] Fahrt durchführen	(TS) Technisches System	-
§ Tätigkeit des Tf im Regelbetrieb		
- Fahrtätigkeit im Regelbetrieb	Manueller Fahrbetrieb mit Zugbeeinflussung	
- Maßgebliche Fahrerlaubnis über...	Technik	

4.2 Phase 2: Das Störungsszenario bestimmen

Nachdem die Grundparameter in der Phase 1 festgelegt wurden, folgt als nächstes die Bestimmung von Parametern des Störungsszenarios. Als Störungsszenario wird eine großräumige und lang andauernde Störung der Gleisfreimeldeanlage bzw. des Achszählersystems auf der freien Strecke zwischen Zmst A und Zmst B als Beispiel gewählt. Durch diese Störung werden alle Blockabschnitte zwischen Zmst A und Zmst B beim Fdl im BZ als „besetzt“ angezeigt. Die Störung lässt sich nach der regelkonformen Bedienung der System-Grundstellung durch den Fdl aber nicht beheben. Es wird eine voraussichtliche Reparaturdauer von 72 Std. bzw. 3 Betriebstagen erwartet. Der Bahnbetrieb zwischen Zmst A und Zmst B wird voraussichtlich in den nächsten 72 Std. im Störungsbetrieb durchgeführt werden. Der Bereich der betrieblichen Störung hat eine Streckenlänge von ca. 20 km bzw. eine Gleislänge von ca. 40 km, wie die Abbildung 30 zeigt.

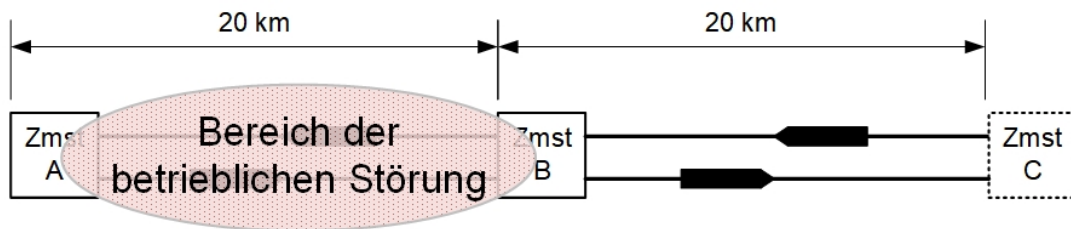


Abbildung 30: Schematische Darstellung von dem Bereich der betrieblichen Störung

Bei der Betrachtung des Betriebs- und Umgebungskontextes wurde kein unmittelbares Anzeichen eines IT-Angriffs festgestellt. Sowohl die aktuelle IT-Bedrohungslage der Systemumgebung als auch das aktuelle IT-Schutzniveau des Systems befinden sich im Niveau „Basis“. Dadurch kann das aktuelle IT-Manipulationspotenzial nach der Manipulationsmatrix in Tabelle 22 mit der Skala „Sehr gering“ eingestuft werden. Der entsprechende Verstärkungsfaktor zu der Skala „Sehr gering“ beträgt nach Tabelle 24 einen Faktorwert von 1,0. Das bedeutet, dass das Betriebsrisiko in dem vorliegenden Szenario nicht durch das IT-Manipulationspotenzial zusätzlich beeinflusst wird.

Da die Realisierung einer sicheren Durchführung der Zugfahrt in der Bewertungssystematik durch das generische Funktionsmodell abgebildet wurde, ist es bei der Ermittlung des Betriebsrisikos im Störungsbetrieb notwendig, zunächst den maßgeblichen Akteur jeder generischen Betriebsfunktion nach dem Störungsszenario zu bestimmen. Aufgrund der vorliegenden Störung von Gleisfreimeldeanlagen kann die Betriebsfunktion [F2] Abstandhaltung sichern nicht durch das technische System realisiert werden. Die Betriebsfunktion Abstandhaltung fällt daher während der Störung unter die Verantwortung des Fdl und wird mit dem Verfahren Räumungsprüfung realisiert. Da alle Signale im Störungsbereich die Hauptsignalfunktion besitzen, werden sie während der Störung Halt anzeigen. Bei der Durchführung der Fahrten im Störungsbetrieb muss der Tf daher an allen haltzeigenden Signalen vorbeifahren. Die entsprechende Fahrerlaubnis zum Vorbeifahren am

haltzeigenden Signal wird dann vom Fdl per Befehl an Tf erteilt. Dadurch fällt die Betriebsfunktion [F4] Fahrerlaubnis bereitstellen ebenfalls unter die Verantwortung des Fdl.

Falls die Zugfahrt mit einer ausgeschalteten Zugbeeinflussung durch den Störungsbereich vom Tf durchgeführt wird, dann liegt die Betriebsfunktion [F7] Fahrt durchführen in jedem Fall in der Verantwortung des Tf. Auch wenn die Zugfahrt zwischen den Signalen teilweise unter Überwachung der Zugbeeinflussung durchgeführt wird, muss der Tf trotzdem zum Vorbeifahren am haltzeigenden Signal bei PZB die Befehlstaste bewusst betätigen. Dadurch wird der Tf nach den Regeln in Kapitel 3.4.2.2 stets als maßgeblicher Akteur für die Betriebsfunktion [F7] Fahrt durchführen in dem vorliegenden Störungsszenario angesehen. Es befinden sich zwar Bahnübergänge auf der freien Strecke zwischen Zmst A und Zmst B, die werden aber in dem vorliegenden Beispiel alle fahrzeugbewirkt [130] eingeschaltet. Demnach ist die Betriebsfunktion [F3] Bahnübergang sichern nicht von der Störung betroffen und wird weiterhin technisch gesichert.

Letztendlich wird der maßgebliche Akteur hinsichtlich der Betriebsfunktionen [F2] Abstandhaltung sichern, [F4] Fahrerlaubnis bereitstellen und [F7] Fahrt durchführen vom technischen System im Regelbetrieb auf den Menschen im vorliegenden Störungsszenario gewechselt haben. Der Rest der Betriebsfunktionen im Funktionsmodell bleibt weiterhin in der Verantwortung des technischen Systems. Eine Übersicht der wesentlichen Parameter des vorliegenden Störungsszenarios befindet sich in Tabelle 33.

Tabelle 33: Parameter eines Störungsszenarios

Parameter	Wert	Einheit
§ Funktionsmodell	(Maßgeblicher Akteur)	
- [F1] Fahrweg sichern	(TS) Technisches System	-
- [F2] Abstandhaltung sichern	(Fdl) Fahrdienstleiter	-
- [F3] Bahnübergang sichern	(TS) Technisches System	-
- [F4] Fahrerlaubnis bereitstellen	(Fdl) Fahrdienstleiter	-
- [F5] Geschwindigkeit signalisieren	(TS) Technisches System	-
- [F6] Brems- & Antriebskräfte bereitstellen	(TS) Technisches System	-
- [F7] Fahrt durchführen	(Tf) Triebfahrzeugführer	-
§ Größe des betrieblichen Störungsbereichs		
- Streckenlänge im Störungsbetrieb	20	km
- Anzahl der Streckengleise	2	Streckengleis
- Gleislänge im Störungsbetrieb	40	km
§ Voraussichtliche Dauer im Störungsbetrieb	72	Std.
§ Aktuelles IT-Manipulationspotenzial		
- Aktuelle Bedrohungslage der Systemumgebung	Basis	-
- Aktuelles IT-Schutzniveau des Systems	Basis	-
- Aktuelles IT-Manipulationspotenzial	Sehr gering	-
- Verstärkungsfaktor	1,0	-

4.3 Phase 3: Qualität der Konzeptvariante ermitteln

Die Variante des Rückfallebenenkonzepts wird in der Phase 3 durch Anwendung der Bewertungssystematik bewertet. Für die Beispielrechnung wird eine Konzeptvariante mit den folgenden Parameterwerten ausgewählt:

- Mittlere Beförderungsgeschwindigkeit von 40 km/h im Störungsbereich.
- Betriebsdichte von 2 Züge/Std. je Richtung bzw. 4 Züge/Std. alle Richtungen.
- Die maximale Dauer der Handlung je Fdl im Störungsbetrieb beträgt 8 Std. pro Schicht.
- Der Tf erhält die Fahrerlaubnis durch den Befehl vom Fdl und betätigt anschließend die Befehlstaste zur Vorbeifahrt am haltzeigenden Signal.
- Der Zug bekommt bei der Vorbeifahrt an einem haltzeigenden Ks-Signal wegen der Befehlstaste keine 1000 Hz-Beeinflussung. Die 500 Hz-Beeinflussung ist weiterhin aktiv und wird vom Zug gelesen.

Der Gedanke hinter dieser Konzeptvariante ist folgende: Aufgrund des dichten Abstands von 1,5 km zwischen den haltzeigenden Signalen sollte der Tf die Zugfahrt zum Zweck des Fahrkomforts mit einer homogenen Fahrweise durchgeführt werden. Um eine ständige Beschleunigung und Abbremsung während der Fahrt zu vermeiden, wird eine mittlere Beförderungsgeschwindigkeit von 40 km/h gewählt. Die Geschwindigkeit von 40 km/h entspricht dem Mittelwert der Überwachungsgeschwindigkeiten eines aktiven PZB 500 Hz-Magnets von der oberen Zugart (45 km/h) und der mittleren Zugart (35 km/h). Mit dieser Geschwindigkeit kann der Tf nach dem Vorbeifahren an einem aktiven 500 Hz-Magnet bis zum kommenden haltzeigenden Signal bzw. zum kommenden aktiven 2000 Hz-Magnet heranfahren, ohne zwangsgebremst zu werden.

Mit der Wahl einer Beförderungsgeschwindigkeit von 40 km/h wird die Betriebsdichte zudem begrenzt. Da keine weitere Zmst zwischen dem Zmst A und Zmst B vorhanden ist, kann die Räumungsprüfung nur in Zmst A oder Zmst B erfolgen. Bei einer Gleislänge von 20 km pro Richtungsgleis im Störungsbereich benötigt ein Zug mit 40 km/h zwischen Zmst A und Zmst B eine Reisezeit von 30 Minuten. Das bedeutet auch, dass in diesen 30 Minuten keine weitere Fahrt auf demselben Streckenabschnitt zwischen Zmst A und Zmst B stattfinden kann. Demzufolge kann mit der Auswahl der Beförderungsgeschwindigkeit von 40 km/h im Teilbereich des betrachteten Fdl-Steuerbereichs zwischen der Zmst A und der Zmst B nur eine maximale Betriebsdichte von 2 Züge/Std. je Richtung im Störungsbetrieb realisiert werden. Im Gegensatz dazu wird angenommen, dass die Betriebsdichte und die Beförderungsgeschwindigkeit im Teilbereich des betrachteten Fdl-Steuerbereichs zwischen der Zmst B und der Zmst C, welcher von der Störung nicht betroffen ist und sich im Regelbetrieb befindet, weiterhin wie planmäßig bei 5 Züge/Std. je Richtung und 100 km/h bleiben werden, wie die Zusammenfassung der Betriebsparameter in Tabelle 34 zeigt.

Tabelle 34: Rechenbeispiel einer Konzeptvariante – Teil 1

Struktur der Bewertungssystematik	Teilbereich des betrachteten Fdl-Steuerbereichs im		Einheit
	Störungsbetrieb (Zmst A - Zmst B)	Regelbetrieb (Zmst B - Zmst C)	
1 - [Betriebsparameter]			
Streckenlänge	20	20	km
Betriebsdichte pro Streckengleis	2	5	Zug/Std.
Anzahl der Streckengleise	2	2	-
Betriebsdichte alle Streckengleise	4	10	Zug/Std.
Mittlere Beförderungsgeschwindigkeit	40	100	km/h
Voraussichtliche Dauer der Störung	72	72	Std.

Nachdem die Betriebsparameter der Konzeptvariante festgelegt wurden, erfolgt als nächster Schritt bei der Bewertung die Ermittlung des Versagenspotenzials des Funktionsmodells. Das Versagenspotenzial eines Funktionsmodells wird nach dem Akteur technisches System und dem Akteur Mensch getrennt ermittelt. Nach dem Funktionsmodell hat der Akteur technisches System im Teilbereich mit Störungsbetrieb die Verantwortung für insgesamt vier generische Betriebsfunktionen. Dazu gehören: [F1] Fahrweg sichern, [F3] Bahnübergang sichern, [F5] Geschwindigkeit signalisieren und [F6] Brems- & Antriebskräfte bereitstellen, wie die Tabelle 35 zeigt.

Tabelle 35: Rechenbeispiel einer Konzeptvariante – Teil 2

Struktur der Bewertungssystematik	Teilbereich des betrachteten Fdl-Steuerbereichs im		Einheit
	Störungsbetrieb (Zmst A - Zmst B)	Regelbetrieb (Zmst B - Zmst C)	
2 - [Funktionsmodell]			
[F1] Fahrweg sichern	(TS) Technisches System	(TS) Technisches System	-
[F2] Abstandhaltung sichern	(Fdl) Fahrdienstleiter	(TS) Technisches System	-
[F3] Bahnübergang sichern	(TS) Technisches System	(TS) Technisches System	-
[F4] Fahrerlaubnis bereitstellen	(Fdl) Fahrdienstleiter	(TS) Technisches System	-
[F5] Geschwindigkeit signalisieren	(TS) Technisches System	(TS) Technisches System	-
[F6] Brems- & Antrieb bereitstellen	(TS) Technisches System	(TS) Technisches System	-
[F7] Fahrt durchführen	(Tf) Triebfahrzeugführer	(TS) Technisches System	-
3 - [Versagenspotenzial]			
3-1 Akteur Technik			
Versagensrate pro Betriebsfunktion	1,00E-09	1,00E-09	Versagen/ Betriebsstd.
Anzahl der Betriebsfunktionen	4	7	-
Versagenspotenzial des Funktionsmodells (Akteur Technik)	4,00E-09	7,00E-09	Versagen/ Betriebsstd.

Angesichts der höheren Betrachtungsebene des Funktionsmodells sowie zum Zweck der Beispielrechnung wird hier eine Basisversagensrate von 1E-09 Versagen/Betriebsstunde gemäß der CSM-Verordnung [20] für alle Betriebsfunktionen angenommen, die in der Verantwortung des technischen Systems liegen. Dadurch erhält das Funktionsmodell im Teilbereich mit Störungsbetrieb (Zmst A - Zmst B) ein Versagenspotenzial in Höhe von 4,00E-09 Versagen/Betriebsstunde von den technischen Systemen. Im Gegensatz dazu hat das technische

System im Teilbereich mit Regelbetrieb (Zmst B - Zmst C) die Verantwortung für alle sieben Betriebsfunktionen. Das gesamte Versagenspotenzial des Funktionsmodells im Teilbereich mit Regelbetrieb in Höhe von $7,00E-09$ Versagen/Betriebsstunde ergibt sich dann direkt aus der Summe aller sieben Betriebsfunktionen, wie die Ergebnisse in Tabelle 35 zeigen.

Sobald das Versagenspotenzial des Funktionsmodells von den technischen Systemen für den Teilbereich im Störungsbetrieb und den Teilbereich im Regelbetrieb bestimmt wurde, folgt als nächstes die Ermittlung des Versagenspotenzials des Funktionsmodells aus den menschlichen Akteuren im Teilbereich mit Störungsbetrieb. Da im Teilbereich mit Regelbetrieb das technische System für alle Betriebsfunktionen die Verantwortung hat, ist eine Ermittlung des menschlichen Versagenspotenzials in diesem Bereich nach Konzept der Bewertungssystematik nicht erforderlich. Bei der Ermittlung des Versagenspotenzials von Menschen werden der Akteur Fdl und der Akteur Tf getrennt behandelt:

Das Versagenspotenzial des Fdl wird auslastungsbedingt durch den Punktestand der Einflussfaktoren Dauer der Handlung (Tabelle 14), Umfang der Handlung (Tabelle 15) sowie die Intensität der Handlung (Tabelle 16) bestimmt. Bei einer maximalen Dauer der Handlung von 8 Std. vom Fdl im Störungsbetrieb erhält der Einflussfaktor Dauer der Handlung in der Stunde 8 der Handlung nach Tabelle 14 einen Punktestand von 2,5 nach der Gewichtung. Da der Fdl im Teilbereich mit Störungsbetrieb nach dem Funktionsmodell für zwei Betriebsfunktionen verantwortlich ist, ohne Zusatzaufgabe, erhält der Einflussfaktor Umfang der Handlung nach Tabelle 15 einen Punktestand von 3,0 nach der Gewichtung. Bei der Bestimmung der Intensität der Handlung ist als Erstes die Anzahl der Funktionsabläufe pro Std. zu ermitteln. Bei einer Taktzeit von 30 Minuten und einer Reisezeit von 30 Minuten im Teilbereich mit Störungsbetrieb wird nach dem Konzept des Funktionsablaufs in Kapitel 3.4.2.3.2 ein Funktionsablauf per Zugfahrt im Störungsbetrieb benötigt. Mit einer Betriebsdichte von 4 Züge/Std. alle Richtungen ergibt sich nach der Formel (12) eine Summe von 4 Funktionsabläufen/Std. im Teilbereich mit Störungsbetrieb. Der Einflussfaktor Intensität der Handlung erhält mit 4 Funktionsabläufen/Std. nach Tabelle 16 einen Punktestand von 3,0 nach der Gewichtung.

Dadurch erhält der Fdl in der Stunde 8 der Handlung im vorliegenden Störungsszenario eine Punktesumme der Auslastung in Höhe von 9 Punkten. Bei einem Punktestand von 9 ergibt sich nach Tabelle 17 eine Versagenswahrscheinlichkeit des Fdl in Höhe von $3,16E-05$ Versagen/Handlungsablauf in der Stunde 8 der Handlung. Da der Fdl im Teilbereich mit Störungsbetrieb für zwei Betriebsfunktionen verantwortlich ist, enthält das Funktionsmodell ein Versagenspotenzial von $6,32E-05$ Versagen/Funktionsablauf aus dem menschlichen Akteur Fdl, wie die Tabelle 36 zeigt. Hier ist jedoch zu beachten, dass dieses Versagenspotenzial in Höhe von $6,32E-05$ Versagen/Funktionsablauf aus dem Fdl lediglich für die Stunde 8 der Handlung vom Fdl gültig ist. Da der Auslastungspunktestand des Fdl nach Tabelle 14 von der Dauer der Handlung des Fdl abhängig ist, ändert sich das Versagenspotenzial des Funktionsmodells des Fdl mit der Dauer des Fdl im Störungsbetrieb. Für die Ermittlung des Betriebsrisikos über einen längeren Zeitraum muss das Versagenspotenzial des Fdl in jeder

betrachteten Stunde neu bestimmt werden. Wegen der Ähnlichkeit des Vorgehens wird die Ableitung des Versagenspotenzials hier in der Beispielrechnung nicht für jede betrachtete Stunde wiederholt. Das Betriebsrisiko der 72 Stunden Störungsbetrieb des vorliegenden Beispiels wurde aber anhand des Versagenspotenzials der einzelnen Stunde korrekt berechnet und dann anschließend nach der Formel (10) kumulativ ermittelt.

Tabelle 36: Rechenbeispiel einer Konzeptvariante – Teil 3

Struktur der Bewertungssystematik	Teilbereich des betrachteten Fdl-Steuerbereichs im		Einheit
3 - [Versagenspotenzial]	Störungsbetrieb (Zmst A - Zmst B)	Regelbetrieb (Zmst B - Zmst C)	
3-2 Akteur Fdl			
Faktor 1: Dauer der Handlung			
Max. Dauer in der Störung	8	-	Std.
Gewichtungsfaktor zu Faktor 1	0,5	-	-
Punktestand Faktor 1	2,5	-	-
Faktor 2: Umfang der Handlung			
Anzahl der Betriebsfunktionen	2	-	-
Zusatzaufgabe vorhanden?	Nein	-	-
Gewichtungsfaktor zu Faktor 2	1,50	-	-
Punktestand Faktor 2	3	-	-
Faktor 3: Intensität der Handlung			
Funktionsablauf pro Fahrt	1	-	-
Funktionsablauf pro Std.	4	-	-
Gewichtungsfaktor zu Faktor 3	1,00	-	-
Punktestand Faktor 3	3	-	-
Punktesumme Auslastung Fdl	9	-	-
Versagenswahrscheinlichkeit pro Betriebsfunktion	3,16E-05	-	Versagen/Ha.
Versagenspotenzial des Funktionsmodells (Akteur Fdl)	6,32E-05	-	Versagen/Fa.

Im Gegensatz zum Versagenspotenzial des Fdl hat das Versagenspotenzial des Tf in der Bewertungssystematik keine Abhängigkeit zu der Dauer der Handlung des Tf, wie es bereits in Kapitel 3.4.2.3.3 begründet wurde. Das Versagenspotenzial des Tf im Teilbereich mit Störungsbetrieb wird nach der Änderung dessen Fahrtätigkeit und dessen Fahrerlaubnistätigkeit zwischen dem Regel- und Störungsbetrieb bestimmt. Bei der Fahrtätigkeit wird die Zugfahrt im Regelbetrieb in dem vorliegenden Szenario vom Tf manuell unter der PZB Überwachung durchgeführt. Dadurch erhält der Tf nach Tabelle 18 einen Auslastungspunkt von 3 Punkten für seine Fahrtätigkeit im Regelbetrieb. Bei der Fahrerlaubnistätigkeit wird die maßgebliche Fahrerlaubnis im Regelbetrieb dem Tf über ein technisches System übermittelt. Daher wird die Auslastung des Tf nach Tabelle 18 mit dem Stand von 1 Auslastungspunkt bewertet. Insgesamt wird die Auslastung des Tf im Regelbetrieb angesichts dessen Fahrtätigkeit und dessen Fahrerlaubnistätigkeit mit einer Summe von 4 Punkten bewertet.

Aufgrund der Störung wird die maßgebliche Fahrerlaubnis im Teilbereich mit Störung vom Fdl per Befehl an Tf übermittelt. Dadurch wird die Auslastung des Tf angesichts dessen Fahrerlaubnistätigkeit nach Tabelle 19 auf den Stand von 3 Auslastungspunkten erhöht. Da die Zugbeeinflussung in der vorliegenden Konzeptvariante trotz der Störung weiterhin zum Teil aktiv ist, bleibt die Auslastung des Tf angesichts dessen Fahrtätigkeit nach Tabelle 19 unverändert mit 3 Auslastungspunkten, wie im Regelbetrieb. Insgesamt ergibt sich für den Tf im Teilbereich mit Störung eine Summe von 6 Auslastungspunkten. Durch die Punkterhöhung der Auslastungspunkte von 4 Punkten im Regelbetrieb auf 6 Punkte im Störungsbetrieb kann die Versagenswahrscheinlichkeit des Tf im Teilbereich mit der Störung nach Tabelle 20 in Höhe von $3,16E-06$ Versagen/Handlungsablauf bei einem Punktanstieg von 2 Punkten ermittelt werden. Da im Funktionsmodell des Teilbereichs mit Störungsbetrieb nur eine Betriebsfunktion in der Verantwortung des Tf liegt, beträgt das Versagenspotenzial des Funktionsmodells bezüglich des menschlichen Akteurs Tf ebenfalls den gleichen Wert in Höhe von $3,16E-06$ Versagen/Funktionsablauf, wie die Zusammenfassung in Tabelle 37 zeigt.

Tabelle 37: Rechenbeispiel einer Konzeptvariante – Teil 4

Struktur der Bewertungssystematik	Teilbereich des betrachteten Fdl-Steuerbereichs im		Einheit
3 - [Versagenspotenzial]	Störungsbetrieb (Zmst A - Zmst B)	Regelbetrieb (Zmst B - Zmst C)	
3-3 Akteur Tf			
Anzahl der Betriebsfunktionen	1	-	-
Fahrtätigkeit im Regelbetrieb	Manueller Fahrbetrieb mit Zugbeeinflussung	-	-
Fahrerlaubnis im Regelbetrieb über	Technik	-	-
Fahrtätigkeit im Störungsbetrieb	Manueller Fahrbetrieb mit Zugbeeinflussung	-	-
Fahrerlaubnis im Störungsbetrieb über	Befehl	-	-
Versagenswahrscheinlichkeit pro Betriebsfunktion	$3,16E-06$	-	Versagen/Ha.
Versagenspotenzial des Funktionsmodells (Akteur Tf)	$3,16E-06$	-	Versagen/Fa.

Nachdem das Versagenspotenzial des Funktionsmodells getrennt nach den Akteuren Tf und Fdl ermittelt wurde, ist als nächster Schritt die Anzahl der Versagen des gesamten Funktionsmodells zu bestimmen, sowohl für den Teilbereich im Störungsbetrieb als auch für den Teilbereich im Regelbetrieb. Die Anzahl der Versagen des technischen Systems lässt sich als Produkt der Summe der Betriebsstunde und des Versagenspotenzials im Funktionsmodell darstellen. Die Summe der Betriebsstunde des technischen Systems ist nach den Betriebsparametern der Teilbereiche zu bestimmen. Anhand der Formel (13) wird die gleiche Summe der Betriebsstunde in Höhe von 2 Betriebsstunde/Std. für die beiden Teilbereichen ausgerechnet. Bei einem Versagenspotenzial des technischen Systems von $7,00E-09$ Versagen/Betriebsstunde im Teilbereich mit Regelbetrieb ergibt sich eine Anzahl der Versagen in Höhe von $1,40E-08$ Versagen/Std. Die Anzahl der Versagen des technischen Systems im

Teilbereich mit Störungsbetrieb in Höhe von $8,00E-09$ Versagen/Std. lässt sich in gleicher Weise aus dem Versagenspotenzial des technischen Systems ($4,00E-09$ Versagen/Betriebsstunde) und dessen Summe der Betriebsstunde (2 Betriebsstunde/Std.) berechnen.

Um die Anzahl der Versagen des gesamten Funktionsmodells in dem Teilbereich mit Störungsbetrieb zu bestimmen, muss neben dem technischen System auch die Anzahl der Versagen der menschlichen Akteure ermittelt werden. Die Anzahl der Versagen der menschlichen Akteure lässt sich als Produkt des Versagenspotenzials im Funktionsmodell pro Funktionsablauf und der Anzahl der Funktionsabläufe pro Std. beschreiben. Das Versagenspotenzial der menschlichen Akteure im Funktionsmodell in der Stunde 8 der Handlung vom Fdl in Höhe von $6,64E-05$ Versagen/Funktionsablauf setzt sich aus dem Versagenspotenzial des Fdl und dem Versagenspotenzial des Tf, welches beim Fdl $6,32E-05$ Versagen/Funktionsablauf und beim Tf $3,16E-06$ Versagen/Funktionsablauf beträgt. Anschließend wird die Anzahl der Funktionsabläufe pro Std. anhand der Formel (12) ermittelt. Die Anzahl der Funktionsabläufe beträgt unter den vorliegenden Betriebsparametern im Teilbereich mit Störungsbetrieb 4 Funktionsabläufe pro Std.

Letztendlich lässt sich die Anzahl der Versagen der menschlichen Akteure bei der achten Handlungsstunde des Fdl im Störungsbetrieb als Produkt der beiden Parameter in Höhe von $2,66E-04$ Versagen/Std. bestimmen. Die Anzahl der Versagen des gesamten Funktionsmodells, zusammengesetzt aus denen des Akteurs Mensch und denen des Akteurs technisches System, beträgt im Teilbereich mit Störungsbetrieb in der Stunde 8 der Handlung vom Fdl ebenfalls $2,66E-04$ Versagen/Std., da die Anzahl der Versagen des technischen Systems in Höhe von $8,00E-09$ Versagen/Std. zu klein ist und deshalb keine Auswirkung auf das Ergebnis bei der Addition hat. Die Anzahl der Versagen des gesamten Funktionsmodells im Teilbereich mit Regelbetrieb hat dann eine Summe von $1,40E-08$ Versagen/Std.

Die gesamte Summe der Versagen des vorliegenden Störungsszenarios mit einer vsl. Störungsdauer von 72 Std. muss dann aus dem Ergebnis der einzelnen Stunde kumulativ summiert werden, da sich die Anzahl der Versagen im Teilbereich mit Störung bei einer Änderung der Handlungsstunde vom Fdl ebenfalls ändert. An dieser Stelle soll der Rechenvorgang für die kumulative Berechnung nicht dargestellt werden. Wie das Ergebnis in Tabelle 38 zeigt, wird in dem betrachteten Fdl-Steuerbereich mit der Anwendung dieser Konzeptvariante in dem vorliegenden 72 Std. Störungsszenario voraussichtlich im Teilbereich mit Störungsbetrieb (Zmst A - Zmst B) $1,10E-02$ Versagen und im Teilbereich mit Regelbetrieb (Zmst B - Zmst C) $1,01E-06$ Versagen erwartet.

Tabelle 38: Rechenbeispiel einer Konzeptvariante – Teil 5

Struktur der Bewertungssystematik	Teilbereich des betrachteten Fdl-Steuerbereichs im		Einheit
4 - [Anzahl der Versagen]	Störungsbetrieb (Zmst A - Zmst B)	Regelbetrieb (Zmst B - Zmst C)	
4-1 Akteur Technik			
Summe Betriebsstunde pro Std.	2,00	2,00	Betriebsstd./Std.
Anzahl der Versagen von dem technischen System pro Std.	8,00E-09	1,40E-08	Versagen/Std.
Anzahl der Versagen von dem technischen System bei 72 Std.	5,76E-07	1,01E-06	Versagen/72 Std.
4-2 Akteur Mensch			
Funktionsablauf pro Std.	4	-	Fa./Std.
Anzahl der Versagen von Menschen (Fdl + Tf) in der Stunde 8 der Handlung vom Fdl im Störungsbetrieb	2,66E-04	-	Versagen/Std.
Anzahl der Versagen von Menschen (Fdl + Tf) bei 72 Std. Betrieb	1,10E-02	-	Versagen/72 Std.
Summe von Technik & Mensch			
Anzahl der Versagen eines Funktionsmodells in der Stunde 8 der Handlung vom Fdl im Störungsbetrieb	2,66E-04	1,40E-08	Versagen/Std.
Anzahl der Versagen eines Funktionsmodells bei 72 Std. Betrieb	1,10E-02	1,01E-06	Versagen/72 Std.

Nach der Anzahl der Versagen ist nach der Struktur der Bewertungssystematik als nächstes das IT-Manipulationspotenzial zu bestimmen. Dieser Verstärkungsfaktor wurde bereits in Kapitel 4.2 im Rahmen der Beschreibung vom Störungsszenario bestimmt. Da kein unmittelbares Anzeichen eines IT-Angriffs festgestellt werden kann, befindet sich sowohl die aktuelle IT-Bedrohungslage der Systemumgebung als auch das aktuelle IT-Schutzniveau des Systems im dem Niveau „Basis“. Nach der Manipulationsmatrix in Tabelle 22 wird das aktuelle IT-Manipulationspotenzial mit der Skala „Sehr gering“ eingestuft. Der entsprechende Verstärkungsfaktor zu der Skala „Sehr gering“ hat nach Tabelle 24 einen Faktorwert von 1,0. Das bedeutet, dass das Betriebsrisiko in dem vorliegenden Szenario nicht zusätzlich durch das IT-Manipulationspotenzial beeinflusst wird.

Als nächster Schritt der Bewertung wird der Reduktionsfaktor bestimmt, da das Eintreten eines Versagens nicht immer zu einem Unfall führen wird. Bei einer Betriebsdichte von 2 Züge/Std. je Richtung im Teilbereich mit Störungsbetrieb (Zmst A - Zmst B) kann nach Tabelle 27 ein Reduktionsfaktor in Höhe von 0,14 ermittelt werden. Im Vergleich dazu liegt der Reduktionsfaktor im Teilbereich mit Regelbetrieb (Zmst B - Zmst C) mit einer Betriebsdichte von 5 Züge/Std. nach Tabelle 27 bei 0,44.

Als letzter Schritt der Bestimmung des Betriebsrisikos muss nach dem Risikomodell noch das maßgebliche Schadensausmaß eines Versagens eingeschätzt werden. Basierend auf der von Menschen übernommenen Betriebsfunktionen [F2] Abstandhaltung sichern und [F4] Fahrerlaubnis bereitstellen wird der Zusammenstoß als maßgebliche Unfallart für den

Teilbereich im Störungsbetrieb angesehen. Die gleiche Unfallart wird in der vorliegenden Beispielrechnung ebenfalls für den Teilbereich mit Regelbetrieb als maßgeblich angenommen. Aufgrund des Mischverkehrs auf der Strecke wird die Unfallkombination GR-RZ / RZ-RZ im Fall eines Zusammenstoßes bestimmt. Bei der Festlegung der Unfallgeschwindigkeit wird hier die Annahme getroffen, dass die Unfallgeschwindigkeit in den beiden Teilbereichen jeweils dessen Beförderungsgeschwindigkeit entspricht. Dadurch liegt die Beförderungsgeschwindigkeit des Teilbereichs im Störungsbetrieb mit 40 km/h in der Geschwindigkeitsklasse 2 ($V \leq 40$ km/h) und die Beförderungsgeschwindigkeit des Teilbereichs im Regelbetrieb mit 100 km/h in der Geschwindigkeitsklasse 4 ($80 < V \leq 120$ km/h).

Zusammenfassend ergibt sich nach der Zuordnungstabelle im Anhang C die Unfallklasse D mit 0,1 Opfer/Versagen im Teilbereich mit Störungsbetrieb und die Unfallklasse G mit 3 Opfer/Versagen im Teilbereich mit Regelbetrieb, wie die Tabelle 39 zeigt.

Tabelle 39: Rechenbeispiel einer Konzeptvariante – Teil 6

Struktur der Bewertungssystematik	Teilbereich des betrachteten Fdl-Steuerbereichs im		Einheit
5 - [IT-Manipulationspotenzial]	Störungsbetrieb (Zmst A - Zmst B)	Regelbetrieb (Zmst B - Zmst C)	
Bedrohungslage der Systemumgebung	Basis	Basis	-
IT-Schutzniveau des Systems	Basis	Basis	-
IT-Manipulationspotenzial	sehr gering	sehr gering	-
Verstärkungsfaktor	1,0	1,0	-
6 - [Reduktionsfaktor]	Störungsbetrieb	Regelbetrieb	
Reduktionsfaktor	0,14	0,44	-
7 - [Schadensausmaß]	Störungsbetrieb	Regelbetrieb	
Unfallart	Zusammenstoß	Zusammenstoß	-
Unfallkombination	GZ-RZ / RZ-RZ	GZ-RZ / RZ-RZ	-
Unfallgeschwindigkeit	Klasse 2 ($V \leq 40$)	Klasse 4 ($80 < V \leq 120$)	km/h
Opferzahl	Klasse D (0,1)	Klasse G (3)	Opfer/ Versagen

Nachdem alle Parameterwerte bestimmt wurden, ergibt sich das Ergebnis des Betriebsrisikos nach der Formel (8) aus dem Produkt von Anzahl der Versagen, IT-Manipulationspotenzial, Reduktionsfaktor und Schadensausmaß des Unfalls. Wie die folgende Beispielberechnung in Tabelle 40 zeigt, beträgt das Betriebsrisiko im Teilbereich mit Störungsbetrieb in der Stunde 8 der Handlung vom Fdl im Störungsbetrieb $3,73\text{E-}06$ Opfer/Std. Im Vergleich dazu liegt das Betriebsrisiko im Teilbereich mit Regelbetrieb pro Stunde bei $1,87\text{E-}08$ Opfer/Std. und somit deutlich niedriger.

Tabelle 40: Beispielberechnung des Betriebsrisiko pro Stunde

§ Betriebsrisiko im Teilbereich mit Störungsbetrieb in der Stunde 8 der Handlung vom Fdl							
Anzahl der Versagen		IT-Manipulations-potenzial		Reduktions-faktor		Schadensausmaß des Unfalls	Betriebsrisiko
2,66E-04	*	1,0	*	0,14	*	0,1	= 3,73E-06
[Versagen/Std.]		[-]		[-]		[Opfer/Versagen]	[Opfer/Std.]
§ Betriebsrisiko im Teilbereich mit Regelbetrieb pro Stunde							
Anzahl der Versagen		IT-Manipulations-potenzial		Reduktions-faktor		Schadensausmaß des Unfalls	Betriebsrisiko
1,40E-08	*	1,0	*	0,44	*	3	= 1,87E-08
[Versagen/Std.]		[-]		[-]		[Opfer/Versagen]	[Opfer/Std.]

Das Betriebsrisiko unter der Anwendung des vorliegenden Rückfallebenenkonzepts während der vsl. 72 Stunden Störung lässt sich ebenfalls getrennt nach den Teilbereichen ausrechnen. Wie die folgende Berechnung zeigt, beträgt das Betriebsrisiko im Teilbereich mit Störung (Zmst A - Zmst B) bei einem 72 Std. Störungsbetrieb 1,55E-04 Opfer/72 Std. Im Vergleich dazu liegt das Betriebsrisiko im Teilbereich mit Regelbetrieb (Zmst B - Zmst C) bei einem 72 Std. Störungsbetrieb bei 1,34E-06 Opfer/72 Std. Das gesamte Betriebsrisiko aus den beiden Teilbereichen des betrachteten Fdl-Steuerbereichs nach der Formel (9) beträgt dann 1,56E-04 Opfer/72 Stunde mit der Anwendung des Rückfallebenenkonzepts, wie die Beispielberechnung in Tabelle 41 zeigt.

Tabelle 41: Beispielberechnung des Betriebsrisikos bei 72 Std. Betrieb

Betriebsrisiko im Teilbereich mit Störungsbetrieb bei 72 Std. Störungsbetrieb							
Anzahl der Versagen		IT-Manipulations-potenzial		Reduktions-faktor		Schadensausmaß des Unfalls	Betriebsrisiko (BR _{BS})
1,10E-02	*	1,0	*	0,14	*	0,1	= 1,55E-04
[Versagen/72 Std.]		[-]		[-]		[Opfer/Versagen]	[Opfer/72 Std.]
Betriebsrisiko im Teilbereich mit Regelbetrieb bei 72 Std. Regelbetrieb							
Anzahl der Versagen		IT-Manipulations-potenzial		Reduktions-faktor		Schadensausmaß des Unfalls	Betriebsrisiko (BR _{BR})
1,01E-06	*	1,0	*	0,44	*	3	= 1,34E-06
[Versagen/72 Std.]		[-]		[-]		[Opfer/Versagen]	[Opfer/72 Std.]
Betriebsrisikos in dem gesamten Fdl-Steuerbereich über 72 Std. (BR _B = BR _{BS} + BR _{BR})						=	1,56E-04
							[Opfer/72 Std.]

Um die Ergebnisse der Bewertung anschaulich darstellen zu können, werden die Ergebnisse anschließend in Qualitätsindize umgewandelt. Wie es bereits in Kapitel 3.3.2 berechnet wurde, hat der hier betrachtete Fdl-Steuerbereich mit einer Gleislänge von 80 km einen Risikogrenzwert von 1,87E-02 Opfern/Jahr. Da in der vorliegenden Arbeit ein

Gesamtbetrachtungszeitraum von einem Kalenderjahr gewählt wurde, kann das Betriebsrisiko der vorliegenden Konzeptvariante bei deren Anwendung von 72 Std. in dem Kalenderjahr durch die Erweiterung des Betrachtungszeitraums ebenfalls als $1,56\text{E-}04$ Opfer/Jahr ausgedrückt und interpretiert werden. Der Risikoindex der vorliegenden Konzeptvariante bei 72 Std. in Höhe von 0,83% lässt sich dann nach der Formel (20) als Prozentsatz des Betriebsrisikos ($1,56\text{E-}04$ Opfer/Jahr) und dem Risikogrenzwert in dem betrachteten Fdl-Bereich pro Kalenderjahr ($1,87\text{E-}02$ Opfer/Jahr) darstellen. Unter der Annahme eines planmäßigen Risikoindex im betrachteten Fdl-Steuerbereich in Höhe von 1,25% bei 7300 Std. Regelbetrieb im Jahr¹⁷, lässt sich die spezifische zulässige Anwendungsdauer des vorliegenden Rückfallebenenkonzepts in Höhe von ca. 8520 Stunden nach der Formel (21) ausrechnen.

Bei einer Betriebsdichte von 4 Züge/Std. alle Richtungen und eine Beförderungsgeschwindigkeit von 40 km/h hat der Teilbereich mit Störungsbetrieb ein Leistungsniveau von 160 in der Stunde der Betrachtung. Im Gegensatz dazu hat der Teilbereich mit Regelbetrieb eine Betriebsdichte von 10 Züge/Std. alle Richtungen und eine Beförderungsgeschwindigkeit von 100 km/h, somit ein Leistungsniveau von 1000 in der Stunde der Betrachtung. Das Leistungsniveau der vorliegenden Konzeptvariante in dem gesamten betrachteten Fdl-Steuerbereich lässt sich dann nach der Formel (22) gewichtet nach der Gleislänge aus den beiden Teilbereichen bestimmen. Da die Gleislänge in dem vorliegenden Beispiel in den beiden Teilbereichen identisch ist, ergibt sich das durchschnittliche Leistungsniveau in dem gesamten Fdl-Steuerbereich in Höhe von 580 direkt aus dem Mittelwert des Leistungsniveaus der Teilbereiche. Infolgedessen kann der Leistungsindex bei einem Leistungsniveau von 1000 im Regelbetrieb nach der Formel (23) mit 58% für eine Stunde der Betrachtung bestimmt werden. Da das Leistungsniveau der vorliegenden Konzeptvariante während der 72 Std. sich nicht ändern wird, bleibt das durchschnittliche Leistungsniveau der Konzeptvariante über 72 Std. nach der Formel (24) unverändert bei 58%. Zuletzt hat der betrachtete Fdl-Steuerbereich in dem vorliegenden Störungsszenario nach der Formel (26) einen Verfügbarkeitsindex in Höhe von 50%, da die Gleislänge in dem Teilbereich mit Störungsbetrieb und in dem Teilbereich mit Regelbetrieb identisch ist. Der durchschnittliche Verfügbarkeitsindex über 72 Std. bleibt dann nach der Formel (27) unverändert bei 50%, da die Aufteilung der Gleislänge in den 72 Std. sich nicht geändert hat. Eine Zusammenfassung aller Qualitätsindexe ist in Tabelle 42 zu finden.

¹⁷ Es wird eine Betriebsdauer von 20 Std. am Tag über 365 Tage angenommen. Die Betriebsdichte und die Beförderungsgeschwindigkeit in dem betrachteten Fdl-Steuerbereich betragen wie in dem vorliegenden Beispiel 10 Züge/Std. alle Richtungen sowie 100 km/h.

Tabelle 42: Rechenbeispiel des Qualitätsindex

Struktur der Bewertungssystematik	Teilbereich des betrachteten Fdl-Steuerbereichs im		Einheit
[Risikoindex]	Störungsbetrieb (Zmst A - Zmst B)	Regelbetrieb (Zmst B - Zmst C)	
Betriebsrisiko im betrachteten Fdl-Steuerbereich bei 72 Std. Betrieb im Jahr	1,56E-04		Opfer/Jahr
Angepasster Risikogrenzwert im betrachteten Fdl-Steuerbereich im Jahr	1,87E-02		Opfer/Jahr
Risikoindex ($RI_{Bn, \Delta t=72Std.}$)	0,83		%
Planmäßiger Risikoindex im betrachteten Fdl-Steuerbereich im Jahr	1,25		%
Spezifische zulässige Anwendungsdauer des Rückfallebenenkonzepts im Jahr	ca. 8520		Std.
[Leistungsindex]	Störungsbetrieb	Regelbetrieb	
Leistungsniveau im Teilbereich	160	1000	-
Leistungsniveau im gesamten Fdl-Steuerbereich	580		-
Durchschnittlicher Leistungsindex ($LI_{Bn, \Delta t=72Std.}$)	58		%
[Verfügbarkeitsindex]	Störungsbetrieb	Regelbetrieb	
Gleislänge im Teilbereich	40	40	km
Durchschnittlicher Verfügbarkeitsindex ($VI_{Bn, \Delta t=72Std.}$)	50		%

4.4 Phase 4: Rückfallebenenkonzept gestalten

Je nach der ausgewählten betrieblichen Maßnahmen lässt sich eine Vielzahl von Konzeptvarianten gestalten. Als Lösungsbeispiele für das vorliegende Störungsszenario werden 10 Basisvarianten in Abschnitt 4.4.1 vorgestellt und bewertet. Die Qualität jeder Basisvariante wird in diesem Abschnitt zwar mit einer Anwendungsdauer von über 72 Std. separat betrachtet, was jedoch nicht bedeutet, dass die Basisvarianten bei der Gestaltung von Rückfallebenenkonzepten nicht miteinander kombiniert werden können. Dafür gibt es verschiedene Gründe. Beispielsweise gibt es innerhalb eines Betriebstages unterschiedliche Verkehrszeiten. Beginnend mit der morgendlichen Hauptverkehrszeit (Früh-HVZ), danach die Normalverkehrszeit (NVZ), Abendliche Hauptverkehrszeit (Spät-HVZ), Schwachverkehrszeit (SVZ) und endet mit der Nachtverkehrszeit (NV) [131]. Häufig wird in der Früh-HVZ und Spät-HVZ eine höhere Betriebsdichte, in der NVZ eine mittlere Betriebsdichte und in der SVZ eine niedrige Betriebsdichte erwartet. In der Nachtverkehrszeit ist es je nach Nachfrage unterschiedlich, ob die Zugfahrten stattfinden. So sind auf der Mischverkehrsstrecke mit dem Streckenstandard M 160 in der Nachtverkehrszeit nach der Regelplanung nur Güterzüge vorgesehen [95]. Werden zu den jeweiligen Verkehrszeiten im Störungsbereich z. B. unterschiedliche Betriebsdichte, Beförderungsgeschwindigkeit oder Verkehrsart erwartet, dann ist es sinnvoll, das Rückfallebenenkonzept eines Betriebstages aus mehreren Basisvarianten zusammenzustellen. Als Gestaltungsbeispiel eines Rückfallebenenkonzepts aus den diversen Basisvarianten werden in Kapitel 4.4.2 vier unterschiedliche Rückfallebenenkonzepte vorgestellt und diskutiert. Des Weiteren, um das Rückfallebenenkonzept mit einem übermäßig hohen stündlichen Betriebsrisiko bei der Anwendung ausschließen zu können, wird hier eine durchschnittliche zulässige Anwendungsdauer des Rückfallebenenkonzepts in Höhe von 185 Std./Jahr zum Zeitpunkt der Bewertung ausgewählt. Die Details über das Konzept und die Festlegung der durchschnittlichen zulässigen Anwendungsdauer des Rückfallebenenkonzepts sind in Kapitel 3.3.3 ausgeführt.

4.4.1 Die Basisvariante

Eine Zusammenfassung der 10 Basisvarianten sowie deren Qualitäten befindet sich am Ende des Abschnitts in Tabelle 53. Hier die 10 Basisvarianten (im Folgenden abgekürzt als Variante) im Einzelnen:

4.4.1.1 Basisvariante-1

Die Variante-1 ist die Beispielvariante, die bereits in Kapitel 4.3 als Rechenbeispiel der Bewertungssystematik ausführlich behandelt wurde. Mit einer mittleren Beförderungsgeschwindigkeit von 40 km/h und einer Betriebsdichten von 4 Züge/Std. alle Richtungen ist die Variante-1 zwar die Variante mit dem niedrigsten Leistungsniveau (LI_{Bn} : 58%), hat jedoch auch das niedrigste Risikoniveau (RI_{Bn} : 0,83%). Außerdem ist für diese Variante keine zusätzliche Personalressourcenplanung nötig, da die maximale Dauer der Handlung des Fdl im Störungsbetrieb bei 8 Std. liegt und kein zusätzlicher Fdl zur Aufgabenteilung vorgesehen ist. Aufgrund ihres niedrigen Risikoniveaus hat die Variante-1 eine spezifische zulässige Anwendungsdauer von ca. 8520 Std. bzw. ca. 12 Monate im Jahr in dem vorliegenden Störungsszenario. Da die spezifische zulässige Anwendungsdauer der Variante-1 im Jahr größer als die durchschnittliche zulässige Anwendungsdauer von 185 Std./Jahr ist, kann die Variante-1 zur Anwendung zugelassen werden. Die wesentlichen Parameter und Ergebnisse von Variante-1 sind in Tabelle 43 zu finden.

Tabelle 43: Basisvariante 1

Parameter & Ergebnis	Variante-1	Einheit
Betriebsdichte alle Streckengleise	4	Zug/Std.
Mittlere Beförderungsgeschwindigkeit	40	km/h
(Fdl) Max. Dauer der Handlung in der Störung	8	Std.
(Fdl) Zusätzlicher Fdl zur Aufgabenteilung	Nein	-
Funktionsablauf pro Fahrt	1	Fa.
(Tf) Fahrtätigkeit im Störungsbetrieb	Manueller Fahrbetrieb mit Zugbeeinflussung	-
(Tf) Fahrerlaubnis im Störungsbetrieb über	Befehl	-
Reduktionsfaktor	0,14	-
Unfallkombination	GZ-RZ / RZ-RZ	-
Opferzahl pro Unfall	0,1	Opfer
Voraussichtliche Dauer der Anwendung	72	Std.
Verfügbarkeitsindex (VI_{Bn})	50	%
Leistungsindex (LI_{Bn})	58	%
Risikoindex (RI_{Bn}) bei 72 Std. Betrieb	0,83	%
Spezifische zulässige Anwendungsdauer	ca. 8520	Std./Jahr
Durchschnittliche zulässige Anwendungsdauer	ca. 185	Std./Jahr
Basisvariante anwendbar?	Ja	

4.4.1.2 Basisvariante-2

Basierend auf der Variante-1 wird in der Variante-2 überlegt, die Betriebsdichte im Störungsbereich ohne begleitende Maßnahmen direkt über dispositive oder fahrdienstliche Anweisung von 4 auf 6 Züge/Std. alle Richtungen zu erhöhen. Um jedoch die Betriebsdichte direkt erhöhen zu können, werden nach der Berechnung der Bewertungssystematik zwei Funktionsabläufe pro Zugfahrt im Teilbereich mit Störungsbetrieb benötigt. Der Grund dafür ist, dass die Zugfahrt nur eine Beförderungsgeschwindigkeit von 40 km/h hat und dadurch eine Belegungszeit von 30 Minuten im Störungsbereich erwartet wird. Bei einer Betriebsdichte von 6 Züge/Std. alle Richtungen bzw. 20 Minuten-Takt muss der nachfolgende Zug nach 20 Minuten bereits in den Störungsbereich einfahren, bevor der vorausfahrende Zug den Störungsbereich verlassen hat. D. h., dass eine weitere Räumungsprüfstelle mitten im Störungsbereich zur Erhöhung der Betriebsdichte erforderlich ist. Aufgrund der infrastrukturellen Einschränkung kann diese Variante hier nicht als Lösungsmöglichkeit betrachtet werden. Die wesentlichen Parameter und Ergebnisse von Variante-2 sind in Tabelle 44 zu finden. Die Zahl in Klammern bei der Betriebsdichte weist darauf hin, dass diese Betriebsdichte von 6 Züge/Std. alle Richtungen unter der vorliegenden Gegebenheit nicht realisierbar ist. Trotz einer infrastrukturellen Einschränkung kann diese Variante jedoch verfahrenstechnisch durch die Einrichtung einer temporären Räumungsprüfstelle realisiert werden. Das Konzept einer temporären Räumungsprüfstelle wird in Kapitel 5.2 vorgestellt und diskutiert.



Tabelle 44: Basisvariante 2

Parameter & Ergebnis	Variante-1	Variante-2	Einheit
Betriebsdichte alle Streckengleise	4	(6)	Zug/Std.
Mittlere Beförderungsgeschwindigkeit	40	40	km/h
(Fdl) Max. Dauer der Handlung in der Störung	8	8	Std.
(Fdl) Zusätzlicher Fdl zur Aufgabenteilung	Nein	Nein	-
Funktionsablauf pro Fahrt	1	2	Fa.
(Tf) Fahrtätigkeit im Störungsbetrieb	Manueller Fahrbetrieb mit Zugbeeinflussung	Manueller Fahrbetrieb mit Zugbeeinflussung	-
(Tf) Fahrerlaubnis im Störungsbetrieb über	Befehl	Befehl	-
Reduktionsfaktor	0,14	0,25	-
Unfallkombination	GZ-RZ / RZ-RZ	GZ-RZ / RZ-RZ	-
Opferzahl pro Unfall	0,1	0,1	Opfer
Voraussichtliche Dauer der Anwendung	72	72	Std.
Verfügbarkeitsindex (VI _{Bn})	50	50	%
Leistungsindex (LI _{Bn})	58	62	%
Risikoindex (RI _{Bn}) bei 72 Std. Betrieb	0,83	13,17	%
Spezifische zulässige Anwendungsdauer	ca. 8520	ca. (535)	Std./Jahr
Durchschnittliche zulässige Anwendungsdauer	ca. 185		Std./Jahr
Basisvariante anwendbar?	Ja	Nein	
Grund des Anwendungsverbots	-	Betriebsdichte nicht realisierbar	

4.4.1.3 Basisvariante-3

Durch die Variante-2 wurde gezeigt, dass die Betriebsdichte in einem Störungsbereich erhöht werden kann, wenn die Reisezeit des Zuges kürzer wird. Daher wird in der Variante-3 überlegt, die Beförderungsgeschwindigkeit im Störungsbereich von 40 km/h auf 60 km/h zu erhöhen, um die Betriebsdichte von 6 Züge/Std. alle Richtungen zu ermöglichen. Durch die Erhöhung der Beförderungsgeschwindigkeit wird die Reisezeit im Störungsbereich von 30 Minuten auf 20 Minuten reduziert. Aufgrund der großräumigen Störung und des dichten Abstands von 1,5 km zwischen den Signalen, kann die erwünschte mittlere Beförderungsgeschwindigkeit von 60 km/h aus dem SPFV, SGV und SPNV in der vorliegenden Variante nicht erreicht werden. Wie die Fahrzeitsimulation im Anhang D zeigt, kann in diesem Störungsbereich wegen des Mischverkehrs und der aktiven PZB-Überwachung lediglich eine mittlere Beförderungsgeschwindigkeit von ca. 45 km/h erreicht werden. Aus diesem Grund kann die Variante-3 nicht für das vorliegende Störungsszenario als Lösungsmöglichkeit berücksichtigt werden. Die wesentlichen Parameter und Ergebnisse von Variante-3 befinden sich in Tabelle 45.

Tabelle 45: Basisvariante 3

Parameter & Ergebnis	Variante-2	Variante-3	Einheit
Betriebsdichte alle Streckengleise	(6) 	(6)	Zug/Std.
Mittlere Beförderungsgeschwindigkeit	40 	(60)	km/h
(Fdl) Max. Dauer der Handlung in der Störung	8	8	Std.
(Fdl) Zusätzlicher Fdl zur Aufgabenteilung	Nein	Nein	-
Funktionsablauf pro Fahrt	2	1	Fa.
(Tf) Fahrtfähigkeit im Störungsbetrieb	Manueller Fahrbetrieb mit Zugbeeinflussung	Manueller Fahrbetrieb mit Zugbeeinflussung	-
(Tf) Fahrerlaubnis im Störungsbetrieb über	Befehl	Befehl	-
Reduktionsfaktor	0,25	0,25	-
Unfallkombination	GZ-RZ / RZ-RZ	GZ-RZ / RZ-RZ	-
Opferzahl pro Unfall	0,1	1,0	Opfer
Voraussichtliche Dauer der Anwendung	72	72	Std.
Verfügbarkeitsindex (VI _{Bn})	50	50	%
Leistungsindex (LI _{Bn})	62	68	%
Risikoindex (RI _{Bn}) bei 72 Std. Betrieb	13,17	37,82	%
Spezifische zulässige Anwendungsdauer	(ca. 535)	(ca. 185)	Std./Jahr
Durchschnittliche zulässige Anwendungsdauer	ca. 185		Std./Jahr
Basisvariante anwendbar?	<u>Nein</u>	<u>Nein</u>	
Grund des Anwendungsverbots	Betriebsdichte nicht realisierbar	Geschwindigkeit nicht realisierbar	

4.4.1.4 Basisvariante-4

Wie in der Variante-3 gezeigt wurde, kann weder die Betriebsdichte noch die Beförderungsgeschwindigkeit unter einer aktiven PZB Überwachung signifikant erhöht werden. Daher wird hier in der Variante-4 überlegt, die Zugbeeinflussung im Störungsbereich während der Zugfahrt zu deaktivieren. Die Zugfahrt durch den Störungsbereich wird dann ohne technische Überwachung vom Tf manuell durchgeführt. Die gesetzliche Vorgabe in Deutschland von max. 50 km/h bei der Zugfahrt ohne technische Sicherung im Bereich der EBO wird weder hier noch in den anderen Varianten als Einschränkung berücksichtigt. Zum einen hat die Arbeit den Zweck das Betriebsrisiko eines leistungsfähigen Rückfallebenenkonzeptes für den Fall einer großräumigen und langdauernden Störung zu bewerten, zum anderen kann in dem vorliegenden Beispielszenario keine leistungsfähigere Basisvariante wegen der gesetzlichen Einschränkung von 50 km/h (vgl. 45 km/h bei Variante-3) ermöglicht werden. Ohne die Einschränkung der technischen Überwachung können die Betriebsdichte in der Variante-4 auf 6 Züge/Std. alle Richtungen und die Beförderungsgeschwindigkeit im Störungsbereich auf 60 km/h erhöht werden. Die maximale Dauer der Handlung des Fdl im Störungsbetrieb bleibt unverändert bei 8 Stunden. Die wesentlichen Parameter und Ergebnisse von Variante-4 befinden sich in Tabelle 46.

Tabelle 46: Basisvariante 4

Parameter & Ergebnis	Variante-3	Variante-4	Einheit
Betriebsdichte alle Streckengleise	(6)	6	Zug/Std.
Mittlere Beförderungsgeschwindigkeit	(60)	60	km/h
(Fdl) Max. Dauer der Handlung in der Störung	8	8	Std.
(Fdl) Zusätzlicher Fdl zur Aufgabenteilung	Nein	Nein	-
Funktionsablauf pro Fahrt	1	1	Fa.
(Tf) Fahrtätigkeit im Störungsbetrieb	Manueller Fahrbetrieb mit Zugbeeinflussung	Manueller Fahrbetrieb ohne Zugbeeinflussung	-
(Tf) Fahrerlaubnis im Störungsbetrieb über	Befehl	Befehl	-
Reduktionsfaktor	0,25	0,25	-
Unfallkombination	GZ-RZ / RZ-RZ	GZ-RZ / RZ-RZ	-
Opferzahl pro Unfall	1,0	1,0	Opfer
Voraussichtliche Dauer der Anwendung	72	72	Std.
Verfügbarkeitsindex (VI_{Bn})	50	50	%
Leistungsindex (LI_{Bn})	68	68	%
Risikoindex (RI_{Bn}) bei 72 Std. Betrieb	37,82	41,76	%
Spezifische zulässige Anwendungsdauer	(ca. 185)	(ca. 170)	Std./Jahr
Durchschnittliche zulässige Anwendungsdauer	ca. 185		Std./Jahr
Basisvariante anwendbar?	Nein	Nein	
Grund des Anwendungsverbots	Geschwindigkeit nicht realisierbar	Stündliches Betriebsrisiko zu hoch	

Das Ergebnis der Bewertung zeigt einen besseren Leistungsindex von 68% im Vergleich zu 58% von Variante-1. Das Betriebsrisiko erhöht sich aber im Vergleich zur Variante-1 signifikant von 0,83% auf 41,76%. Daraus ergibt sich die spezifische zulässige

Anwendungsdauer der Variante-4 in Höhe von 170 Std./Jahr, die aber die durchschnittliche zulässige Anwendungsdauer vom Rückfallebenenkonzept in Höhe von 185 Std./Jahr unterschreitet. Demzufolge kann die Variante-4 wegen ihres übermäßig hohen stündlichen Betriebsrisikos nicht zur Anwendung zugelassen werden.

4.4.1.5 Basisvariante-5

Auch wenn das Leistungsniveau des Bahnbetriebs durch die Variante-4 sich von 58% im Gegensatz zu Variante-1 auf 68% verbessert hat, ist das stündliche Betriebsrisiko viel zu hoch und kann nicht angewendet werden. Basierend auf der Variante-4 wird in der Variante-5 versucht, das Betriebsrisiko durch die Reduzierung der maximalen Dauer der Handlung des Fdl im Störungsbetrieb abzusenken. Die maximale Dauer der Handlung des Fdl im Störungsbetrieb wird in der Variante-5 von 8 aufeinanderfolgenden Stunden auf 4 aufeinanderfolgende Stunden reduziert. Das heißt aber nicht, dass der Fdl während einer lang andauernden Störung nach 4 Std. Arbeit direkt Dienstschluss hat. Je nach der Personalressourcenplanung kann es möglich sein, dass z. B. der Fdl eine angemessene Pause einlegt und danach zum Teilbereich mit Störungsbetrieb zurückkehrt. Eine andere Alternative wäre z. B. der Tausch des Steuerbereichs mit dem anderen Fdl, dessen Steuerbereich sich komplett im Regelbetrieb befindet. Wie das Ergebnis in Tabelle 47 zeigt, wird der Risikoindex durch die Anpassung der Arbeitsdauer von 41,76% auf 34,23% reduziert. Infolgedessen wird die spezifische zulässige Anwendungsdauer der Variante-5 auf ca. 205 Std. erhöht, die gerade über die durchschnittliche zulässige Anwendungsdauer liegt. Der Leistungsindex bleibt weiterhin bei 68% aufgrund der unveränderten Betriebsdichte und der Beförderungsgeschwindigkeit. Die wesentlichen Parameter und Ergebnisse von Variante-4 sind in Tabelle 47 zu finden.



Tabelle 47: Basisvariante 5

Parameter & Ergebnis	Variante-4	Variante-5	Einheit
Betriebsdichte alle Streckengleise	6	6	Zug/Std.
Mittlere Beförderungsgeschwindigkeit	60	60	km/h
(Fdl) Max. Dauer der Handlung in der Störung	8	4	Std.
(Fdl) Zusätzlicher Fdl zur Aufgabenteilung	Nein	Nein	-
Funktionsablauf pro Fahrt	1	1	Fa.
(Tf) Fahrtätigkeit im Störungsbetrieb	Manueller Fahrbetrieb <i>ohne</i> Zugbeeinflussung	Manueller Fahrbetrieb <i>ohne</i> Zugbeeinflussung	-
(Tf) Fahrerlaubnis im Störungsbetrieb über	Befehl	Befehl	-
Reduktionsfaktor	0,25	0,25	-
Unfallkombination	GZ-RZ / RZ-RZ	GZ-RZ / RZ-RZ	-
Opferzahl pro Unfall	1,0	1,0	Opfer
Voraussichtliche Dauer der Anwendung	72	72	Std.
Verfügbarkeitsindex (VI _{Bn})	50	50	%
Leistungsindex (LI _{Bn})	68	68	%
Risikoindex (RI _{Bn}) bei 72 Std. Betrieb	41,76	34,23	%
Spezifische zulässige Anwendungsdauer	(ca. 170)	ca. 205	Std./Jahr
Durchschnittliche zulässige Anwendungsdauer	ca. 185		Std./Jahr
Basisvariante anwendbar?	Nein	Ja	
Grund des Anwendungsverbots	Stündliches Betriebsrisiko zu hoch	-	

4.4.1.6 Basisvariante-6

Nach dem das Betriebsrisiko durch die Anpassung der Arbeitsdauer in der Variante-5 erfolgreich reduziert wurde, wird hier in der Variante-6 weiter versucht, das Leistungsniveau der Variante zu erhöhen. Basierend auf der Variante-5 wird die Betriebsdichte in der Variante-6 von 6 auf 8 Züge/Std. alle Richtungen und die Beförderungsgeschwindigkeit von 60 km/h auf 80 km/h weiter erhöht. Das Ergebnis der Bewertung zeigt eine klare Verbesserung des Leistungsniveaus von 68% auf 82%. Jedoch erhält der Fdl durch die Erhöhung der Betriebsdichte auch zusätzliche Auslastung bei der Arbeit. Es hat zur Folge, dass der Risikoindex in der vorliegenden Variante von 34,23% auf 75,17% deutlich angestiegen ist. Dadurch ist die spezifische zulässige Anwendungsdauer der Variante-6 auf ca. 90 Std. stark gesunken, die deutlich unter der durchschnittlichen zulässigen Anwendungsdauer im Jahr liegt. Aufgrund des übermäßig hohen stündlichen Betriebsrisikos kann die Variante-6 nicht zur Anwendung zugelassen werden. Die wesentlichen Parameter und Ergebnisse von Variante-6 sind in Tabelle 48 zu finden.


Tabelle 48: Basisvariante 6

Parameter & Ergebnis	Variante-5	Variante-6	Einheit
Betriebsdichte alle Streckengleise	6 	8	Zug/Std.
Mittlere Beförderungsgeschwindigkeit	60 	80	km/h
(Fdl) Max. Dauer der Handlung in der Störung	4	4	Std.
(Fdl) Zusätzlicher Fdl zur Aufgabenteilung	Nein	Nein	-
Funktionsablauf pro Fahrt	1	1	Fa.
(Tf) Fahrtätigkeit im Störungsbetrieb	Manueller Fahrbetrieb <i>ohne Zugbeeinflussung</i>	Manueller Fahrbetrieb <i>ohne Zugbeeinflussung</i>	-
(Tf) Fahrerlaubnis im Störungsbetrieb über	Befehl	Befehl	-
Reduktionsfaktor	0,25	0,25	-
Unfallkombination	GZ-RZ / RZ-RZ	GZ-RZ / RZ-RZ	-
Opferzahl pro Unfall	1,0	1,0	Opfer
Voraussichtliche Dauer der Anwendung	72	72	Std.
Verfügbarkeitsindex (VI _{Bn})	50	50	%
Leistungsindex (LI _{Bn})	68	82	%
Risikoindex (RI _{Bn}) bei 72 Std. Betrieb	34,23	75,17	%
Spezifische zulässige Anwendungsdauer	ca. 205	(ca. 90)	Std./Jahr
Durchschnittliche zulässige Anwendungsdauer	ca. 185		Std./Jahr
Basisvariante anwendbar?	Ja	<u>Nein</u>	
Grund des Anwendungsverbots	-	Stündliches Betriebsrisiko zu hoch	

4.4.1.7 Basisvariante-7

Durch die Variante-6 hat sich gezeigt, dass der Anstieg der Betriebsdichte die Auslastung des Akteurs Mensch erhöht und somit zur Erhöhung des Betriebsrisikos führen kann. Es wird daher durch die Variante-7 versucht, die Auslastung der Menschen unter der Einhaltung des Leistungsniveaus wie bei der Variante-6 möglichst zu reduzieren und dadurch auch das Betriebsrisiko abzusenken. Als Ansatz wird hier ein zusätzlicher Fdl zur Aufgabenteilung nach Betriebsrichtung ausgewählt. Eine Aufteilung nach Betriebsrichtung auf einer zweigleisigen Strecke mit dem Richtungsbetrieb hat zu bedeuten, dass ein Fdl nur für die Fahrten in Bezug auf die Fahrerlaubnis zuständig ist, die auf dem ihm zugeteilten Streckengleis verkehren. In dem vorliegenden Beispielszenario wird ein Fdl in Zmst A für die Fahrten auf dem rechten Gleis (Zmst A → Zmst B) und der andere Fdl in Zmst B für die Fahrten auf dem linken Gleis (Zmst B → Zmst A) zuständig sein. Wie das Ergebnis der Bewertung in Tabelle 49 zeigt, kann der Risikoindex der Variante-7 durch den zusätzlichen Fdl signifikant auf 29,03% reduziert werden. Die spezifische zulässige Anwendungsdauer der Variante-7 liegt dann bei ca. 240 Std./Jahr, die die Anforderung einer durchschnittlichen zulässigen Anwendungsdauer von 185 Std./Jahr erfüllt. Der Leistungsindex bleibt damit unverändert bei 82% der Regelleistung. Die wesentlichen Parameter und Ergebnisse von Variante-6 befinden sich in Tabelle 49.

Tabelle 49: Basisvariante 7

Parameter & Ergebnis	Variante-6	Variante-7	Einheit
Betriebsdichte alle Streckengleise	8	8	Zug/Std.
Mittlere Beförderungsgeschwindigkeit	80	80	km/h
(Fdl) Max. Dauer der Handlung in der Störung	4	4	Std.
(Fdl) Zusätzlicher Fdl zur Aufgabenteilung	Nein 	Ja	-
Funktionsablauf pro Fahrt	1	1	Fa.
(Tf) Fahrtätigkeit im Störungsbetrieb	Manueller Fahrbetrieb ohne Zugbeeinflussung	Manueller Fahrbetrieb ohne Zugbeeinflussung	-
(Tf) Fahrerlaubnis im Störungsbetrieb über	Befehl	Befehl	-
Reduktionsfaktor	0,25	0,25	-
Unfallkombination	GZ-RZ / RZ-RZ	GZ-RZ / RZ-RZ	-
Opferzahl pro Unfall	1,0	1,0	Opfer
Voraussichtliche Dauer der Anwendung	72	72	Std.
Verfügbarkeitsindex (VI _{Bn})	50	50	%
Leistungsindex (LI _{Bn})	82	82	%
Risikoindex (RI _{Bn}) bei 72 Std. Betrieb	75,17	29,03	%
Spezifische zulässige Anwendungsdauer	(ca. 90)	ca. 240	Std./Jahr
Durchschnittliche zulässige Anwendungsdauer	ca. 185		Std./Jahr
Basisvariante anwendbar?	Nein	Ja	
Grund des Anwendungsverbots	Stündliches Betriebsrisiko zu hoch	-	

4.4.1.8 Basisvariante-8

Mit der Variante-7 endet die Vorgehensweise der leistungsorientierten Variantengestaltung, da eine weitere Erhöhung der Betriebsdichte auf 10 Züge/Std. alle Richtungen nur mit einer parallelen Erhöhung der Beförderungsgeschwindigkeit auf 100 km/h in dem vorliegenden Beispielszenario möglich ist. Sobald die Beförderungsgeschwindigkeit über 80 km/h liegt, wird das Schadensausmaß um eine weitere Unfallklasse auf 3 Opfer/Versagen steigen, egal ob mit oder ohne die Erhöhung der Betriebsdichte. Der Risikoindex der neuen Variante mit 100 km/h wird dann auf über 90% steigen und ist somit nicht anwendbar. Analog zur Variante-7 wird hier in der Variante-8 das Betriebsrisiko der vorhandenen Variante-5 durch einen zusätzlichen Fdl zur Aufgabenteilung reduziert. Die maximale Dauer der Handlung des Fdl im Störungsbetrieb bleibt wie in der Variante-5 weiterhin bei 4 Stunden. Wie die Ergebnisse in Tabelle 50 zeigen, kann in dieser Variante der Risikoindex durch einen weiteren Fdl zur Aufgabenteilung von 34,23% auf unter 21,77% reduziert werden. Somit steigt die spezifische zulässige Anwendungsdauer der Variante-8 auf ca. 325 Std./Jahr.

Tabelle 50: Basisvariante 8

Parameter & Ergebnis	Variante-5	Variante-8	Einheit
Betriebsdichte alle Streckengleise	6	6	Zug/Std.
Mittlere Beförderungsgeschwindigkeit	60	60	km/h
(Fdl) Max. Dauer der Handlung in der Störung	4	4	Std.
(Fdl) Zusätzlicher Fdl zur Aufgabenteilung	Nein	Ja	-
Funktionsablauf pro Fahrt	1	1	Fa.
(Tf) Fahrtätigkeit im Störungsbetrieb	Manueller Fahrbetrieb <i>ohne Zugbeeinflussung</i>	Manueller Fahrbetrieb <i>ohne Zugbeeinflussung</i>	-
(Tf) Fahrerlaubnis im Störungsbetrieb über	Befehl	Befehl	-
Reduktionsfaktor	0,25	0,25	-
Unfallkombination	GZ-RZ / RZ-RZ	GZ-RZ / RZ-RZ	-
Opferzahl pro Unfall	1,0	1,0	Opfer
Voraussichtliche Dauer der Anwendung	72	72	Std.
Verfügbarkeitsindex (VI _{Bn})	50	50	%
Leistungsindex (LI _{Bn})	68	68	%
Risikoindex (RI _{Bn}) bei 72 Std. Betrieb	34,23	21,77	%
Spezifische zulässige Anwendungsdauer	ca. 205	ca. 325	Std./Jahr
Durchschnittliche zulässige Anwendungsdauer	ca. 185		Std./Jahr
Basisvariante anwendbar?	Ja	Ja	
Grund des Anwendungsverbots	-	-	

4.4.1.9 Basisvariante-9

Es wird bisher in der Variante-1 angenommen, dass die Zugfahrt nach der Störung zum Teil weiterhin unter der Überwachung der Zugbeeinflussung durchgeführt wird. Jedoch ist es möglich, dass die Funktionen der streckenseitigen Sicherungstechnik einschließlich der PZB-Magneten wegen Reparaturen zeitweise komplett außer Betrieb gesetzt werden müssen. Infolgedessen muss die Zugfahrt ohne Zugbeeinflussung durchgeführt werden. Basierend auf der Variante-1 wird hier in der Variante-9 lediglich die Fahrtätigkeit des Tf auf den manuellen Fahrbetrieb ohne Zugbeeinflussung geändert. Alle anderen Parameter wurden unverändert aus der Variante-1 übernommen. Wie die Ergebnisse in Tabelle 51 zeigen, wird der Risikoindex mit dieser Anpassung von 0,83% auf 0,98% leicht erhöht, die dann eine Reduzierung der spezifischen zulässigen Anwendungsdauer der Variante-9 auf ca. 7240 Std. bzw. ca. 10 Monate zur Folge hat.

Tabelle 51: Basisvariante 9

Parameter & Ergebnis	Variante-1	Variante-9	Einheit
Betriebsdichte alle Streckengleise	4	4	Zug/Std.
Mittlere Beförderungsgeschwindigkeit	40	40	km/h
(Fdl) Max. Dauer der Handlung in der Störung	8	8	Std.
(Fdl) Zusätzlicher Fdl zur Aufgabenteilung	Nein	Nein	-
Funktionsablauf pro Fahrt	1	1	Fa.
(Tf) Fahrtätigkeit im Störungsbetrieb	Manueller Fahrbetrieb mit Zugbeeinflussung	Manueller Fahrbetrieb ohne Zugbeeinflussung	-
(Tf) Fahrerlaubnis im Störungsbetrieb über	Befehl	Befehl	-
Reduktionsfaktor	0,14	0,14	-
Unfallkombination	GZ-RZ / RZ-RZ	GZ-RZ / RZ-RZ	-
Opferzahl pro Unfall	0,1	0,1	Opfer
Voraussichtliche Dauer der Anwendung	72	72	Std.
Verfügbarkeitsindex (VI _{Bn})	50	50	%
Leistungsindex (LI _{Bn})	58	58	%
Risikoindex (RI _{Bn}) bei 72 Std. Betrieb	0,83	0,98	%
Spezifische zulässige Anwendungsdauer	ca. 8520	ca. 7240	Std./Jahr
Durchschnittliche zulässige Anwendungsdauer	ca. 185		Std./Jahr
Basisvariante anwendbar?	Ja	Ja	
Grund des Anwendungsverbots	-	-	

4.4.1.10 Basisvariante-10

Zuletzt sollte durch die Variante-10 gezeigt werden, dass das Betriebsrisiko durch die Bündelung von artgleichen Zügen signifikant reduziert werden kann. Basierend auf der Variante-4, wird die Unfallkombination in der Variante 10 von GZ-RZ/RZ-RZ auf GZ-GZ geändert. Das bedeutet, dass der Teilbereich mit Störungsbetrieb nur von Güterzügen befahren werden darf. Nach Zuordnungstabelle im Anhang C wird bei einem Zusammenstoß zwischen zwei Güterzügen mit einer Unfallgeschwindigkeit von 60 km/h als Schadensausmaß die Unfallklasse D mit 0,1 Opfer erwartet. Im Vergleich dazu wird ein Zusammenstoß bei der gleichen Unfallgeschwindigkeit mit Reisezügen die Unfallklasse F mit 1,0 Opfer erwartet. Der Unterschied der beiden Schadensausmaße liegt dann bei Faktor 10. Wie die Ergebnisse in Tabelle 52 zeigen, kann der Risikoindex mit der Änderung der Verkehrsart von 41,76% auf 4,18% signifikant reduziert werden. Somit steigt die spezifische zulässige Anwendungsdauer der Variante von ca. 170 Std. auf ca. 1700 Std. im Jahr, was deutlich über die durchschnittliche zulässige Anwendungsdauer von ca. 185 Std./Jahr liegt. Diese Variante hat jedoch den Nachteil, dass mit ihrer Anwendung nur Güterzüge im Teilbereich mit Störungsbetrieb verkehrt werden dürfen, was in der Folge zur Beeinträchtigung des Reiseverkehrs auf der Mischverkehrsstrecke führen kann. Es wird daher empfohlen, dass diese Variante im Rahmen eines kombinierten Rückfallebenenkonzepts anzuwenden ist, wie im anschließenden Kapitel 4.4.2 gezeigt wird. Variante-10 ist insbesondere für den Nachtverkehr sinnvoll, da die Strecke zu diesen Zeiten meistens nur von Güterzügen befahren wird.

Tabelle 52: Basisvariante 10

Parameter & Ergebnis	Variante-4	Variante-10	Einheit
Betriebsdichte alle Streckengleise	6	6	Zug/Std.
Mittlere Beförderungsgeschwindigkeit	60	60	km/h
(Fdl) Max. Dauer der Handlung in der Störung	8	8	Std.
(Fdl) Zusätzlicher Fdl zur Aufgabenteilung	Nein	Nein	-
Funktionsablauf pro Fahrt	1	1	Fa.
(Tf) Fahrtätigkeit im Störungsbetrieb	Manueller Fahrbetrieb <i>ohne</i> Zugbeeinflussung	Manueller Fahrbetrieb <i>ohne</i> Zugbeeinflussung	-
(Tf) Fahrerlaubnis im Störungsbetrieb über	Befehl	Befehl	-
Reduktionsfaktor	0,25	0,25	-
Unfallkombination	GZ-RZ / RZ-RZ	GZ-GZ	-
Opferzahl pro Unfall	1,0	0,1	Opfer
Voraussichtliche Dauer der Anwendung	72	72	Std.
Verfügbarkeitsindex (VI _{Bn})	50	50	%
Leistungsindex (LI _{Bn})	68	74	%
Risikoindex (RI _{Bn}) bei 72 Std. Betrieb	41,76	4,18	%
Spezifische zulässige Anwendungsdauer	(ca. 170)	ca. 1700	Std./Jahr
Durchschnittliche zulässige Anwendungsdauer	ca. 185		Std./Jahr
Basisvariante anwendbar?	<u>Nein</u>	<u>Ja</u>	
Grund des Anwendungsverbots	Stündliches Betriebsrisiko zu hoch	-	

4.4.1.11 Zusammenfassung

Die wesentlichen Parameter der 10 Basisvarianten sowie ihre Qualitäten werden in Tabelle 53 zusammengefasst.

Tabelle 53: Vergleich von Basisvarianten

Variante	Anwendbarkeit der Variante	RI _{Bn}	LI _{Bn}	V _B	D _{AR}	S	Mit/Ohne Zugbeeinflussung	Max. Dauer der Handlung des Fdl	Mit einem zusätzlichen Fdl	Spezifische zulässige Anwendungsdauer
Var-1	Ja	0,83	58	40	4	0,10	Mit	8	Nein	8520
Var-2	<i>Nein</i>	13,17	62	40	(6)	0,10	Mit	8	Nein	(535)
Var-3	<i>Nein</i>	37,82	68	(60)	(6)	1,00	Mit	8	Nein	(185)
Var-4	<i>Nein</i>	41,76	68	60	6	1,00	Ohne	8	Nein	(170)
Var-5	Ja	34,23	68	60	6	1,00	Ohne	4	Nein	205
Var-6	<i>Nein</i>	75,17	82	80	8	1,00	Ohne	4	Nein	(90)
Var-7	Ja	29,03	82	80	8	1,00	Ohne	4	Ja	240
Var-8	Ja	21,77	68	60	6	1,00	Ohne	4	Ja	325
Var-9	Ja	0,98	58	40	4	0,10	Ohne	8	Nein	7240
Var-10	Ja	4,18	68	60	6 ^{*G}	0,10	Ohne	8	Nein	1700

RI_{Bn} (%): Risikoindex im gesamten Fdl-Steuerbereich bei 72 Std. Störung

LI_{Bn} (%): Leistungsindex im gesamten Fdl-Steuerbereich bei 72 Std. Störung

V_B (km/h): Mittlere Beförderungsgeschwindigkeit im Teilbereich mit Störungsbetrieb

D_{AR} (Züge/Std. alle Richtungen): Mittlere Betriebsdichte pro Std. alle Richtungen im Teilbereich mit Störungsbetrieb

S (Opfer/Versagen): Schadensausmaß

(Zahlen in Klammern): In der vorliegenden infrastrukturellen sowie verfahrenstechnischen Gegebenheit nicht realisierbar

(Zahlen in Klammern, kursiv): Die Anforderung einer durchschnittlichen zulässigen Anwendungsdauer vom Rückfallebenenkonzept in Höhe von 185 Std./Jahr wurde nicht erfüllt.

*G: Nur Güterzüge

Wie die Ergebnisse zeigen, kann der Bahnbetrieb in der vorliegenden großräumigen Störung mit den Varianten Variante-1 und Variante-9, welche eine niedrige Betriebsdichte von 4 Züge/Std. alle Richtungen und eine mittlere Beförderungsgeschwindigkeit von 40 km/h haben, über ein ganzes Jahr durchgeführt werden. Um jedoch die Betriebsdichte von 4 auf 6 Züge/Std. alle Richtungen steigern zu können, muss die infrastrukturelle und verfahrenstechnische Einschränkung in dem vorliegenden Beispiel überwunden werden. Daher kann die Variante-2 in dem vorliegenden Beispiel nicht als Lösungsvariante angesehen werden. Jedoch kann z. B. temporär eine Räumungsprüfstelle verfahrenstechnisch eingerichtet werden, dann ist eine direkte Erhöhung der Betriebsdichte ohne Deaktivierung der Zugbeeinflussung möglich. Es ist aber zu beachten, dass eine Erhöhung der Betriebsdichte und der Beförderungsgeschwindigkeit durch die Deaktivierung der Zugbeeinflussung die Erhöhung des Betriebsrisikos als Folge haben kann, wie das Ergebnis von Variante-4 zeigt. Infolgedessen wird in der Variante-5 bis Variante-10 versucht, durch die Anpassung und Kombination der unterschiedlichen Parameter das Betriebsrisiko zu reduzieren. Als Ergebnis zeigen die Variante-7 und Variante-8 zwar das niedrigste Betriebsrisiko im Leistungsbereich (LI_{Bn}) ab 68% bei Mischverkehr, was jedoch nur mit dem zusätzlichen Fdl und der Reduzierung der Handlungsdauer des Fdl im Störungsbetrieb

zu realisieren ist. Zuletzt wird in der Variante-10 eine effektive Maßnahme zur Reduzierung des Betriebsrisikos durch die Bündelung artgleicher Züge auf der Mischverkehrsstrecke aufgezeigt. Zur Gestaltung des Rückfallebenenkonzepts im Fall einer großräumigen und lang andauernden Störung können nach den Verkehrszeiten am Tag unterschiedliche Basisvarianten angewendet werden. Diese Möglichkeit der Gestaltung von Rückfallebenenkonzepten nach den Verkehrszeiten und dem Betriebsprogramm wird in dem anschließenden Abschnitt durch vier kombinierte Rückfallebenenkonzepte beispielhaft dargestellt und diskutiert.

4.4.2 Das kombinierte Rückfallebenenkonzept

Um ein Rückfallebenenkonzept nach den Verkehrszeiten für das vorliegende Störungsszenario gestalten zu können, werden als erstes die Verkehrszeiten im Störungsbereich festgelegt. Nach den Grundparametern des vorliegenden Beispiels hat die Strecke den Streckenstandard M 160. Zum Bestimmen der Verkehrszeiten wird die planerische Tagesganglinie bzw. das Betriebsprogramm des Streckenstandard M 160 aus der Richtlinie 413 des DB Netz AG zugrunde gelegt [95]. Wie die Abbildung 31 zeigt, wird aus der oberen Grenze und der unteren Grenze der Tagesganglinie¹⁸ von M 160, wie in der Richtlinie 413 vorgegeben, eine durchschnittliche Tagesganglinie abgeleitet.

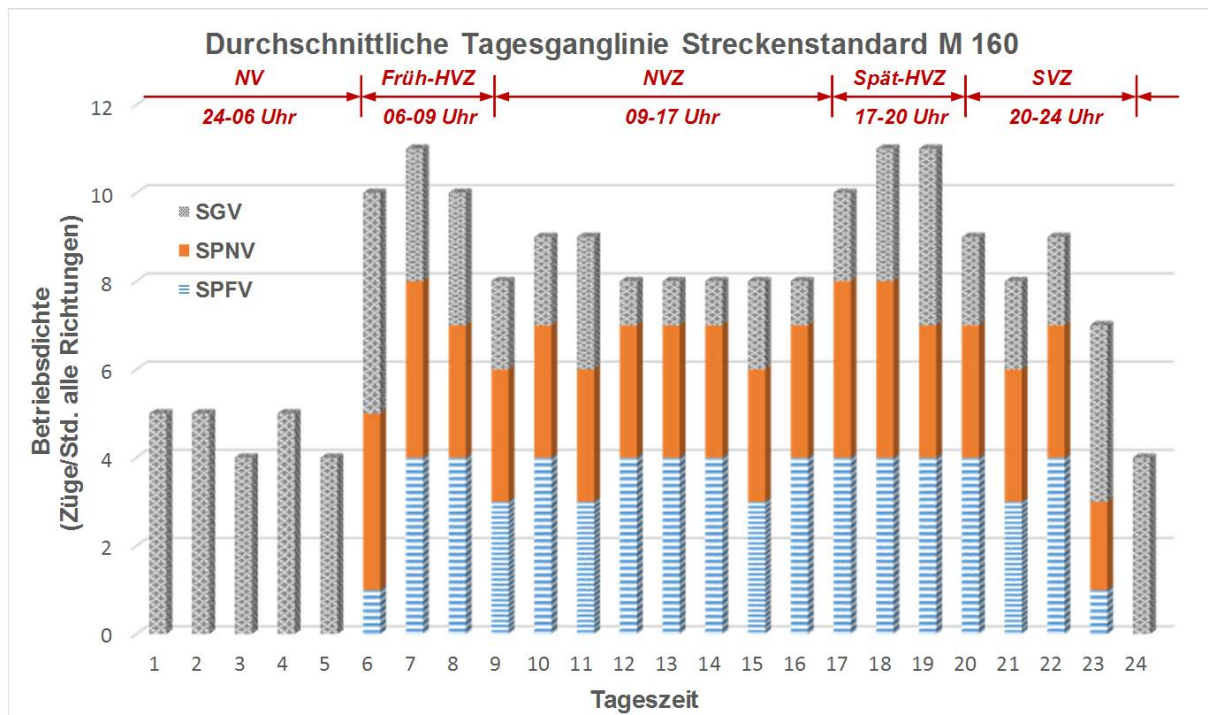


Abbildung 31: Die Verkehrszeiten und Tagesganglinie von Streckenstandard M 160 nach [95]

Aus der durchschnittlichen Tageslinie lässt sich entnehmen, dass die morgendliche Hauptverkehrszeit der Strecke M 160 in den Tageszeiten 06-09 Uhr und die abendliche Hauptverkehrszeit zwischen 17-20 Uhr liegt. Die Normalverkehrszeit liegt dann zwischen der Früh-HVZ und der Spät-HVZ von 09-17 Uhr. Nach der Spät-HVZ wird die Betriebsdichte reduziert und es folgt die Schwachverkehrszeit von 20 Uhr bis 24 Uhr. Letztlich wird in der Nachtverkehrszeit die Betriebsdichte weiter gesenkt und außerdem ist nur Güterverkehr auf der Strecke vorgesehen. Basierend auf dieser Aufteilung von Verkehrszeiten werden hier vier Rückfallebenenkonzepte (im Folgenden abgekürzt als Konzept) für das vorliegende Störungsszenario aus den unterschiedlichen Basisvarianten zusammengestellt und diskutiert. Es werden nur die Basisvarianten, bei der Gestaltung der kombinierten Rückfallebenenkonzepte angewendet, bei denen kein Anwendungsverbot vorliegt.

¹⁸ Die obere Grenze und die untere Grenze der Tagesganglinie von M 160 befinden sich im Anhang E.

4.4.2.1 Kombiniertes Rückfallebenenkonzept A

Bei der Gestaltung vom Konzept A wird das Ziel verfolgt, dass die untere Grenze des Tagesprogramms auf der Strecke M 160 auch im Teilbereich mit Störungsbetrieb eingehalten wird. Allerdings sollte das Betriebsrisiko trotz dieser Anforderung gering gehalten werden. Das Konzept soll dabei nicht nur der Mindestleistung entsprechen, sondern auch über einen sehr langen Zeitraum in der Störung angewendet werden können. Wie im Anhang E zu sehen, hat die Strecke M 160 als Betriebsprogramm in 24 Stunden eine untere Grenze von 60 Reisezügen und 20 Güterzügen alle Richtungen. Da auf der Strecke in der Nachtverkehrszeit von 24 bis 06 Uhr lediglich die Güterzüge verkehren sollen, können die Reisezüge nur in den anderen Verkehrszeiten untergebracht werden. Demzufolge kann die Anforderung von 60 Reisezügen am Tag nur mit einer Betriebsdichte von 4 Züge/Std. alle Richtungen in den verfügbaren 18 Std. Tageszeit erreicht werden.

Als mögliche Variante mit einer Mindestbetriebsdichte von 4 Züge/Std. alle Richtungen und zugleich einem niedrigen Betriebsrisiko kommen die Variante-1 und die Variante-9 in Frage. Wie die Tabelle 54 zeigt, wird hier in der Früh-HVZ und NVZ die Variante-1, in der Spät-HVZ und SVZ die Variante-9 als Konzept ausgewählt. Im Grunde kann die Variante-9 in der Spät-HVZ und SVZ auch durch die Variante-1 mit einem niedrigeren Betriebsrisiko ersetzt werden. Es wird aber hier die Annahme getroffen, dass die technische Sicherung bzw. die Zugbeeinflussung in der Spät-HVZ und SVZ wegen Reparaturarbeit zeitweilig außer Betrieb gesetzt werden muss. Dadurch kommt die Variante-9 zum Einsatz. Als Betriebsprogramm wird in der Früh-HVZ und Spät-HVZ lediglich der Reiseverkehr vorgesehen. Auch in der NVZ und SVZ wird der Fokus auf den Reiseverkehr gelegt. Es wird ein Mischverkehr mit 3 Reisezüge und 1 Güterzug pro Std. alle Richtungen geplant. Dadurch ergibt sich eine Anzahl von 60 Reisezügen am Tag, die genau der Anforderung der unteren Grenze entspricht.

Wegen der Priorisierung von Reiseverkehr zwischen 06-24 Uhr werden die Güterzüge in die Nachtverkehrszeit verschoben. Um eine höhere Betriebsdichte von Güterzügen zu ermöglichen, wird die Variante-10 mit einem reinen Güterverkehr in der Nachtverkehrszeit angewendet. Insgesamt können mit dem Betriebsprogramm 48 Güterzüge am Tag erreicht werden, davon 36 Fahrten in der Nachtverkehrszeit, womit das Ergebnis deutlich höher ist als die untere Grenze des Streckenstandards von 20 Güterzügen am Tag. Eine Absenkung der Betriebsdichte in der Nachtverkehrszeit ist in dem vorliegenden Szenario nicht vorgesehen, da das Betriebsrisiko vom Konzept A trotz der höheren Betriebsdichte von Güterverkehr in der Nachtverkehr noch recht niedrig ist. Der Risikoindex vom Konzept A beträgt 1,82% bei 72 Std. Störungsbetrieb. Das entspricht einer spezifischen zulässigen Anwendungsdauer des Rückfallebenenkonzept von ca. 3965 Std. bzw. ca. 6 Monaten. Die mittlere Beförderungsgeschwindigkeit im Teilbereich mit Störungsbetrieb beträgt 45 km/h. Der Leistungsindex im gesamten Fdl-Steuerbereich liegt dann bei 60%.

Im Anhang F befindet sich der detaillierte stündliche Ablaufplan der Varianten des 72 Std. Störungsbetriebs. Da die Anwendungsdauer einer Variante länger als die variantenabhängige

max. Arbeitsdauer des Fdl sein kann, wird bei der Erstellung des stündlichen Ablaufplans auch die Fdl-Schicht sowie die aktuellen Arbeitsstunden der Schicht zusammenhängend berücksichtigt. Da die Störung zu jedem beliebigen Zeitpunkt eintreten kann, wird daher bei der Erstellung des Ablaufplans die Annahme getroffen, dass die erste Stunde der Störung auf dem Beginn der Früh-HVZ um 06 Uhr und die letzte Stunde der 72 Std. Störung auf dem Ende der NV um 05 Uhr liegt.

Tabelle 54: Variantenablauf und Ergebnisse des Rückfallebenenkonzepts A

Verkehrszeiten	Tageszeit	Basisvariante	Verkehrsart	Betriebsdichte (Züge/Std. alle Richtungen)	davon RZ	davon GZ
Früh-HVZ	06-09 Uhr	Variante-1	Reiseverkehr	4	4	0
NVZ	09-17 Uhr	Variante-1	Mischverkehr	4	3	1
Spät-HVZ	17-20 Uhr	Variante-9	Reiseverkehr	4	4	0
SVZ	20-24 Uhr	Variante-9	Mischverkehr	4	3	1
NV	24-06 Uhr	Variante-10	Güterverkehr	6	0	6
Summe der Züge pro 24 Std.		davon Reisezüge pro 24 Std.		davon Güterzüge pro 24 Std.		
108 Züge		60 Reisezüge		48 Güterzüge		
Risikoindex bei 72 Std. Störungsbetrieb	Spezifische zulässige Anwendungsdauer des Konzepts		Leistungsindex bei 72 Std. Störungsbetrieb	Mittlere Beförderungs- geschwindigkeit		
1,82%	ca. 3965 Std./Jahr		60%	45 km/h		

4.4.2.2 Kombiniertes Rückfallebenenkonzept B

Ausgehend vom Konzept A wird die Betriebsdichte hier im Konzept B in der Früh-HVZ und Spät-HVZ von 4 auf 6 Züge/Std. alle Richtungen sowie die Beförderungsgeschwindigkeit von 40 auf 60 km/h erhöht. Die Verkehrsart in der HVZ bleibt aber weiterhin unverändert bei Reiseverkehr. Durch diese Konzeptänderung wird die Anzahl der Reisezüge von 60 auf 72 Reisezüge am Tag erhöht. Bei einer Betriebsdichte von 6 Züge/Std. alle Richtungen und einer Beförderungsgeschwindigkeit von 60 km/h kommen im Grunde die Variante-4 bis Variante-8 bei der Anwendung in Frage. Die Variante-4 und Variante-6 können hier wegen des übermäßigen Anstiegs des stündlichen Betriebsrisikos bei der Konzeptgestaltung nicht berücksichtigt werden. Variante-7 und Variante-8 sind zwar angesichts ihres niedrigeren Betriebsrisikos, besser als die Variante-5, jedoch wird bei den beiden Varianten ein zusätzlicher Fdl benötigt. Bei der Gestaltung vom Konzept B wird das Ziel verfolgt, den Aufwand der Personalressourcenplanung trotz der Erhöhung des Leistungsniveaus möglichst gering zu halten. Daher wird hier im Konzept B kein zusätzlicher Fdl zur Aufgabeteilung eingeplant. Eine Reduzierung von Dauer der Handlung im Störungsbetrieb z. B. durch den Tausch des Steuerbereichs mit dem Fdl im Regelbetrieb ist aber erlaubt. Aus diesem Grund wird die Variante-5 bevorzugt. Wie das Ergebnis in Tabelle 55 zeigt, beträgt der Risikoindex des Konzepts B 9,83% bei 72 Std. Störungsbetrieb. Das entspricht umgerechnet einer spezifischen zulässigen Anwendungsdauer von ca. 730 Std. bzw. 1 Monat im Jahr. Der Leistungsindex des Konzepts B erhöht sich durch die Variante-5 nur leicht auf 63% der Regelleistung im gesamten Fdl-Steuerbereich. Die mittlere Beförderungsgeschwindigkeit beträgt im Teilbereich mit Störungsbetrieb dann 50 km/h. Der detaillierte stündliche Ablaufplan der Varianten des 72 Std. Störungsbetriebs ist im Anhang G zu finden.

Tabelle 55: Variantenablauf und Ergebnisse des Rückfallebenenkonzepts B

Verkehrszeiten	Tageszeit	Basisvariante	Verkehrsart	Betriebsdichte (Züge/Std. alle Richtungen)	davon RZ	davon GZ
Früh-HVZ	06-09 Uhr	Variante-5	Reiseverkehr	6	6	0
NVZ	09-17 Uhr	Variante-1	Mischverkehr	4	3	1
Spät-HVZ	17-20 Uhr	Variante-5	Reiseverkehr	6	6	0
SVZ	20-24 Uhr	Variante-1	Mischverkehr	4	3	1
NV	24-06 Uhr	Variante-10	Güterverkehr	6	0	6
Summe der Züge pro 24 Std.		davon Reisezüge pro 24 Std.		davon Güterzüge pro 24 Std.		
120 Züge		72 Reisezüge		48 Güterzüge		
Risikoindex bei 72 Std. Störungsbetrieb		Spezifische zulässige Anwendungsdauer des Konzepts		Leistungsindex bei 72 Std. Störungsbetrieb	Mittlere Beförderungs- geschwindigkeit	
9,83%		ca. 730 Std./Jahr		63%	50 km/h	

4.4.2.3 Kombiniertes Rückfallebenenkonzept C

Ausgehend vom Konzept B, wird hier im Konzept C die Betriebsdichte in der NVZ und der SVZ ebenfalls von 4 auf 6 Züge/Std. alle Richtungen erhöht. Angesichts der insgesamt längeren Betriebsdauer von 12 Std. am Tag in der NVZ und SVZ im Gegensatz zu 6 Std. am Tag in der HVZ, wird hier eine Variante mit einer längeren spezifischen zulässigen Anwendungsdauer bevorzugt. Aus diesem Grund wird anstatt der Variante-5 die Variante-8 in der NVZ und SVZ angewendet. Eine weitere Änderung dem Konzept B gegenüber ist die Umstellung der Verkehrsart auf Mischverkehr zwischen 06 und 24 Uhr. Dadurch wird die Anzahl der Güterzüge in der HVZ von 0 auf 2 Züge/Std. alle Richtungen erhöht. Auch die Anzahl der Güterzüge in der NVZ und SVZ wird von 1 auf 2 Züge/Std. alle Richtungen erhöht. Insgesamt steigt mit dieser Programmänderung die Anzahl der Güterzüge von 60 auf 72 Güterzüge am Tag. Die Anzahl der Reisezüge bleibt aber unverändert bei 72 Reisezüge am Tag. Wie das Ergebnis in Tabelle 56 zeigt, wird der Leistungsindex vom Konzept C durch die Erhöhung der Betriebsdichte und der Beförderungsgeschwindigkeit von 63% auf 68% im gesamten Fdl-Steuerbereich erhöht. Der Risikoindex steigt jedoch parallel von 9,83% auf 19,70% bei 72 Std. Störungsbetrieb, wodurch die spezifische zulässige Anwendungsdauer des Konzepts von ca. 730 auf ca. 365 Std. im Jahr reduziert.

Tabelle 56: Variantenablauf und Ergebnisse des Rückfallebenenkonzepts C

Verkehrszeiten	Tageszeit	Basisvariante	Verkehrsart	Betriebsdichte (Züge/Std. alle Richtungen)	davon RZ	davon GZ
Früh-HVZ	06-09 Uhr	Variante-5	Mischverkehr	6	4	2
NVZ	09-17 Uhr	Variante-8	Mischverkehr	6	4	2
Spät-HVZ	17-20 Uhr	Variante-5	Mischverkehr	6	4	2
SVZ	20-24 Uhr	Variante-8	Mischverkehr	6	4	2
NV	24-06 Uhr	Variante-10	Güterverkehr	6	0	6
Summe der Züge pro 24 Std.		davon Reisezüge pro 24 Std.		davon Güterzüge pro 24 Std.		
144 Züge		72 Reisezüge		72 Güterzüge		
Risikoindex bei 72 Std. Störungsbetrieb		Spezifische zulässige Anwendungsdauer des Konzepts		Leistungsindex bei 72 Std. Störungsbetrieb		Mittlere Beförderungsgeschwindigkeit
19,70%		ca. 365 Std./Jahr		68%		60 km/h

Beim stündlichen Ablaufplan vom Konzept C im Anhang H wird berücksichtigt, dass in der Stunde mit der Variante-8 stets zwei Fdl benötigen werden und deren Dauer der Handlung in der Störung max. 4 aufeinanderfolgende Stunden nicht überschreiten darf. Angesichts der Anwendung von 12 Std./Tag und der max. Dauer der Handlung des Fdl im Störungsbetrieb 4 Std. werden drei Schichten mit je zwei Fdl in den Verkehrszeiten bei der Anwendung der Variante-8 vorgesehen. Bei der Erstellung des Schichtplans im Anhang H wird daher die Regel verfolgt: bei jedem Wechsel von Variante-5 in die Variante-8 die Arbeitszeit der Fdl mit der

Variante-5 frühzeitig zu beenden, auch wenn die 4 Std. Grenze noch nicht erreicht ist. Wie das Wechseln zwischen der Spät-HVZ und der SVZ zeigt, wird der Fdl D in der Spät-HVZ (Variante-5) mit dem Wechseln in die SVZ (Variante-8) frühzeitig von den Fdl E1 und E2 abgelöst. Diese vereinfachte Schichtplanung ist für eine korrekte Berechnung des Betriebsrisikos bei einem solchem Rückfallebenenkonzept notwendig, welches aus den Varianten mit der unterschiedlichen spezifischen zulässigen Anwendungsdauer und der unterschiedlichen Dauer der Handlung des Fdl besteht.

4.4.2.4 Kombiniertes Rückfallebenenkonzept D

Ausgehend von dem Konzept C wird hier in dem Konzept D das Leistungsniveau des Konzepts durch die Erhöhung der Betriebsdichte und der Beförderungsgeschwindigkeit in der HVZ weiter verbessert. Die Betriebsdichte in der Früh-HVZ und Spät-HVZ beträgt nach der Erhöhung 8 Züge/Std. alle Richtungen. Zugleich wird auch die Beförderungsgeschwindigkeit von 60 auf 80 km/h erhöht. Die zusätzlichen Fahrten in der HVZ werden im Konzept D ausschließlich vom Reiseverkehr genutzt. Dadurch wird die Anzahl der Reisezüge von 72 auf 84 Reisezüge am Tag erhöht, während die Summe der Güterzüge bei 72 Güterzügen am Tag unverändert bleibt. Wegen der hohen Betriebsdichte von 8 Züge/Std. alle Richtungen und einer Beförderungsgeschwindigkeit von 80 km/h in der HVZ bleibt die Variante-7 als einzige Option übrig, da die Variante-6 wegen des höheren stündlichen Betriebsrisikos nicht berücksichtigt werden kann.

Wie das Ergebnis in Tabelle 57 zeigt, wird der Leistungsindex vom Konzept D durch diese Konzeptänderung von 68% auf 72% im gesamten Fdl-Steuerbereich erhöht. Der Risikoindex des Konzept D wird allerdings trotz der Erhöhung des Leistungsindex von 19,70% auf 18,57% reduziert. Der Grund für diese Reduzierung ist die Aufteilung der Aufgaben durch einen zusätzlichen Fdl. Dadurch wird die spezifische zulässige Anwendungsdauer von 365 auf 390 Std. im Jahr leicht erhöht. Der Ablaufplan des Konzept D im Anhang I ähnelt dem Ablaufplan vom Konzept C sehr. Der einzige Unterschied liegt in der angewandten Variante und dem zusätzlichen Fdl in der Früh-HVZ und Spät-HVZ. Ansonsten sind beide Ablaufpläne bzw. die Schichtpläne identisch.

Tabelle 57: Variantenablauf und Ergebnisse des Rückfallebenenkonzepts D

Verkehrszeiten	Tageszeit	Basisvariante	Verkehrsart	Betriebsdichte (Züge/Std. alle Richtungen)	davon RZ	davon GZ
Früh-HVZ	06-09 Uhr	Variante-7	Mischverkehr	8	6	2
NVZ	09-17 Uhr	Variante-8	Mischverkehr	6	4	2
Spät-HVZ	17-20 Uhr	Variante-7	Mischverkehr	8	6	2
SVZ	20-24 Uhr	Variante-8	Mischverkehr	6	4	2
NV	24-06 Uhr	Variante-10	Güterverkehr	6	0	6
Summe der Züge pro 24 Std.		davon Reisezüge pro 24 Std.		davon Güterzüge pro 24 Std.		
156 Züge		84 Reisezüge		72 Güterzüge		
Risikoindex bei 72 Std. Störungsbetrieb		Spezifische zulässige Anwendungsdauer des Konzepts		Leistungsindex bei 72 Std. Störungsbetrieb		Mittlere Beförderungs- geschwindigkeit
18,57%		ca. 390 Std./Jahr		72%		65 km/h

4.4.2.5 Zusammenfassung

Durch die vier Beispielkonzepte wurde in dem vorliegenden Abschnitt gezeigt, wie ein Rückfallebenenkonzept aus mehreren Varianten unter der Berücksichtigung der Verkehrszeiten und Fdl-Schicht für ein lang andauerndes Störungsszenario zusammengestellt werden kann. Wie das Ergebnis in Tabelle 58 zeigt, kann mit der Anwendung vom Konzept A in dem vorliegenden Beispielszenario zwar nur ein Leistungsindex von 60% erreicht werden, jedoch mit einer sehr langen spezifischen zulässigen Anwendungsdauer aufgrund des niedrigen Betriebsrisikos. Um das Betriebsrisiko bei einer leistungsorientierten Gestaltung von Rückfallebenenkonzepten möglichst minimieren zu können, wird mit der Erhöhung des Leistungsniveaus zugleich ein ansteigender Aufwand der Personalressourcenplanung erwartet. Während bei dem Konzept A kein zusätzlicher Fdl benötigt und eine max. Dauer der Handlung des Fdl im Störungsbetrieb bis zu 8 aufeinanderfolgende Stunden zugelassen wird, muss die Dauer der Handlung des Fdl in der Früh-HVZ und Spät-HVZ bei dem Konzept B bereits auf 4 aufeinanderfolgende Stunden beschränkt werden. Bei dem Leistungsanstieg vom Konzept B auf Konzept C wird dann die Dauer der Handlung des Fdl in der NVZ und SVZ ebenfalls auf 4 aufeinanderfolgende Stunden eingeschränkt und zusätzlich ein zweiter Fdl in den beiden Verkehrszeiten benötigt. Zuletzt wird bei dem Konzept D der höchste Aufwand bei der Personalressourcenplanung vorgesehen, da die Dauer der Handlung des Fdl in allen Verkehrszeiten außer Nachtverkehrszeit auf 4 aufeinanderfolgende Stunden eingeschränkt und außerdem immer zwei Fdl zu jeder Stunde zwischen 06 und 24 Uhr benötigt werden.

Tabelle 58: Vergleich von Rückfallebenenkonzepten

Ergebnis	Konzept A	Konzept B	Konzept C	Konzept D
Leistungsindex bei 72 Std. Betrieb	60%	63%	68%	72%
Anzahl der Züge pro 24 Std.	108 Züge	120 Züge	144 Züge	156 Züge
Mittlere Beförderungsgeschwindigkeit	45 km/h	50 km/h	60 km/h	65 km/h
Risikoindex bei 72 Std. Betrieb	1,82%	9,83%	19,70%	18,57%
Spezifische zulässige Anwendungsdauer des Konzepts im Jahr	ca. 3965 Std.	ca. 730 Std.	ca. 365 Std.	ca. 390 Std.
Relativer Aufwand der Personalressourcenplanung	klein	mittelmäßig	hoch	sehr hoch

5 Diskussion

5.1 Maßnahmen zur Erhöhung der Betriebsqualität

Je nach Priorität des zu verbessernden Qualitätsmerkmals im Rahmen einer Bewertung, kann die Konzeptvariante durch die Änderung von Betriebsvariablen zur Verbesserung der Sicherheit, des Leistungsniveaus oder der Verfügbarkeit gezielt gesteuert werden. Wird ein bestimmtes Qualitätsmerkmal als Ziel einer betrieblichen Variante gesetzt, dann gibt es folgende Lösungsmöglichkeiten:

- Erhöhung der Sicherheit durch:
 - Minimierung des Schadensausmaßes,
 - Minimierung des menschlichen Versagenspotenzials.
- Erhöhung des Leistungsniveaus durch:
 - Erhöhung der Betriebsdichte,
 - Erhöhung der Beförderungsgeschwindigkeit.
- Erhöhung der Verfügbarkeit durch:
 - Minimierung der Störungsdauer,
 - Minimierung des betrieblichen Störungsbereichs.

Es muss aber beachtet werden, dass die Änderung einer Betriebsvariablen, zwecks Verbesserung eines bestimmten Qualitätsmerkmals, auch negative Auswirkungen auf ein anderes Qualitätsmerkmal ausüben kann. Im folgenden Abschnitt werden die Optimierungsmöglichkeiten von Betriebsqualitäten anhand der betrieblichen Maßnahmen einzeln diskutiert.

5.1.1 Maßnahmen zur Erhöhung der Sicherheit

Um die Sicherheit im Störungsbetrieb zu verbessern, gibt es zwei Vorgehensweisen, eine mittels Minimieren des Schadensausmaßes, die andere durch die Verringerung des menschlichen Versagenspotenzials. Eine Übersicht der Maßnahmen ist in Tabelle 59 zu finden.

Die wirksamste betriebliche Maßnahme zur Minimierung des Schadensausmaßes ist die Anordnung eines Betriebsausfalls im Störungsbereich. Da solange der Betrieb stillsteht, auch kein Schaden entstehen kann. Allerdings hat der Betriebsausfall eine gravierende Auswirkung auf das Leistungsniveau des Bahnbetriebs, da im Störungsbereich keine Zugfahrt stattfinden kann. Eine weitere Maßnahme zum Minimieren des Schadensausmaßes wäre z. B. die Reduzierung der Betriebsgeschwindigkeit. Diese Maßnahme hat den Vorteil, dass der Betrieb nicht stillgelegt werden muss. Der damit verbundene Nachteil ist jedoch die Absenkung des Leistungsniveaus durch die Reduzierung der Betriebsgeschwindigkeit. Eine weitere Maßnahme zum Minimieren des Schadensausmaßes ist z. B. die Bündelung von artgleichen Zügen auf der Mischverkehrsstrecke im Fall einer lang andauernden Störung. Wie die Zuordnungstabelle im Anhang C zeigt, ist das zu erwarteten Schadensausmaß bei einem Unfall mit der Beteiligung eines Reisezugs deutlich höher als bei einem Unfall zwischen zwei Güterzügen in jeder

Geschwindigkeitsklasse und Unfallart. D. h., wird die Verkehrsart im Störungsbereich durch die Bündelung der artgleichen Züge von Mischverkehr auf reinen Güterverkehr umgestellt, dann kann das Betriebsrisiko in den Stunden mit dem reinen Güterverkehr deutlich reduziert werden. Diese Maßnahme erfordert aber die Änderung des Fahrplans. Außerdem kann sie sich negativ auf die Kundenzufriedenheit auswirken, da die Züge evtl. nicht mehr zum gewöhnten Zeitpunkt fahren können – insbesondere im Reiseverkehr.

Tabelle 59: Betriebliche Maßnahmen zur Erhöhung der Sicherheit und deren Konsequenzen

Vorgehensweise	Betriebliche Maßnahmen	Negative Auswirkungen
Minimieren des Schadensausmaßes	→ Reduzierung der Geschwindigkeit	Leistungsniveau
	→ Betriebsausfall	Leistungsniveau
	→ Bündelung von artgleichen Zügen auf der Mischverkehrsstrecke	Kundenzufriedenheit
Minimieren des menschlichen Versagenspotenzials	→ Reduzierung der Dauer der Handlung des Fdl im Störungsbetrieb	Personalressourcenplanung
	→ Zusätzliche Fdl zur Aufgabenteilung	Personalressourcenplanung
	→ Reduzierung der Betriebsdichte	Leistungsniveau
	→ Betriebsausfall	Leistungsniveau
	→ Erhöhung der Beförderungsgeschwindigkeit	Sicherheit

Die zweite Vorgehensweise zur Erhöhung der Sicherheit im Störungsbetrieb ist das Minimieren vom menschlichen Versagenspotenzial. Basierend auf den Einflussfaktoren Dauer, Umfang und Intensität der Handlung kann das Versagenspotenzial von Menschen abgesenkt werden. Dies geschieht z. B. durch die Reduzierung der Dauer der Handlung im Störungsbetrieb, die Aufteilung der Aufgaben zwischen mehreren Fdl im Störungsbetrieb oder die Reduzierung der Betriebsdichte. Mit der Reduzierung der Dauer der Handlung des Fdl im Störungsbetrieb sowie dem Anfordern von zusätzlichen Fdl können jedoch negative Auswirkungen bzw. Herausforderungen auf die Personalressourcenplanung haben. Die Reduzierung der Betriebsdichte bis zum kompletten Betriebsausfall beeinträchtigt aber wiederum das Leistungsniveau im Störungsbereich. Die Verringerung der Intensität von Handlungen muss nicht unbedingt über die Reduzierung der Betriebsdichte erfolgen. In bestimmten Fällen kann die Intensität der Handlung des Fdl ebenfalls durch die Erhöhung der Geschwindigkeit im Störungsbereich reduziert werden. Z. B. wenn die Züge in einem Störungsbereich im 15-Minuten-Takt fahren, aber eine Reisezeit von 30 Minuten haben, dann muss zur Realisierung des 15-Minuten-Takts die Abstandhaltung zwischen den Zügen auf einer Zmst mitten im Störungsbereich von dem Fdl gesichert werden. Diese Handlung von dem Fdl wird aber nicht benötigt, wenn die Reisezeit durch eine Geschwindigkeitserhöhung im Störungsbereich auf z. B. 10 Minuten reduziert werden kann. Bevor der nachfolgende Zug 15 Minuten später in den Störungsbereich einfährt, sollte der vorausfahrende Zug den Störungsbereich bereits verlassen haben. Die Intensität der Handlung des Fdl wird dann aufgrund des ausgefallenden Handlungsbedarfs auf einer Zmst mitten im Störungsbereich reduziert. Allerdings ist zu beachten, dass eine höhere Geschwindigkeit im Fall eines Unfalls auch ein größeres

Schadenspotenzial hat. Dadurch kann die Sicherheit des Bahnbetriebs kontraproduktiv beeinträchtigt werden.

5.1.2 Maßnahmen zur Erhöhung des Leistungsniveaus

Das Leistungsniveau einer Konzeptvariante kann durch die Erhöhung der Betriebsdichte und/oder durch die Erhöhung der Geschwindigkeit im Störungsbereich realisiert werden. Sofern die Kapazitätsgrenze im Bereich der Störung unter der vorliegenden infrastrukturellen oder verfahrenstechnischen Gegebenheit noch nicht erreicht ist, lässt sich die Betriebsdichte ohne begleitende Maßnahmen direkt durch die dispositive oder fahrdienstliche Anweisung erhöhen. Wie z. B. durch die Bündelung von artgleichen Zügen auf der Mischverkehrsstrecke [72].

Ist die Grenze aber bereits erreicht, kann die Betriebsdichte im laufenden Betrieb nur durch eine verfahrenstechnische Änderung weiter erhöht werden. Ein Beispiel dafür ist die Einschränkung der Betriebsdichte aufgrund fehlender Räumungsprüfstellen im Störungsbereich. Da die Räumungsprüfung verfahrenstechnisch nur an der vorhandenen Räumungsprüfstelle durchgeführt werden darf, kann die Betriebsdichte im Falle einer fehlenden Infrastruktur bzw. Räumungsprüfstelle mitten im Störungsbereich dadurch eingeschränkt werden. Infrastrukturell gesehen kann das Einrichten einer echten Räumungsprüfstelle nicht sofort realisiert werden. Es bleibt dann nur die verfahrenstechnische Lösung zum Einrichten einer temporären Räumungsprüfstelle. Das Konzept und der Nutzen einer temporären Räumungsprüfstelle werden anschließend in Kapitel 5.2 behandelt. Unabhängig davon, ob die Betriebsdichte durch eine dispositive oder verfahrenstechnische Maßnahme erhöht wird, hat die Erhöhung der Betriebsdichte immer eine negative Auswirkung auf die Auslastung des Fdl und als Folge dessen auf die Sicherheit des Bahnbetriebs.

Eine weitere Vorgehensweise zur Erhöhung des Leistungsniveaus ist eine Geschwindigkeitserhöhung im Störungsbereich. Eine Geschwindigkeitserhöhung kann auch dispositiv oder fahrdienstlich direkt ohne begleitende Maßnahmen veranlasst werden, sofern die Anweisung die zulässige technische, betriebliche oder strukturelle Grenze noch nicht überschritten hat. Eine weitere Erhöhung der Geschwindigkeit lässt sich nur durch eine Unterlassung der technischen Sicherung realisieren. Ein Beispiel dafür ist der manuelle Fahrbetrieb ohne Zugbeeinflussung. Alle Maßnahmen zur Erhöhung der Geschwindigkeit haben negative Auswirkungen auf die Sicherheit des Bahnbetriebs, da mit der Erhöhung der Geschwindigkeit auch ein größeres Schadenausmaß beim Unfall erwartet wird. Eine Übersicht der Maßnahmen ist in Tabelle 60 zu finden.

Tabelle 60: Betriebliche Maßnahmen zur Erhöhung des Leistungsniveaus und deren Konsequenzen

Vorgehensweise	Betriebliche Maßnahmen	Negative Auswirkungen
Erhöhung der Betriebsdichte	→ Bündelung von artgleichen Zügen auf der Mischverkehrsstrecke	Sicherheit
	→ Einrichten von temporären Räumungsprüfstellen	Sicherheit
Erhöhung der Geschwindigkeit	→ (Wird dispositiv oder fahrdienstlich ohne begleitende Maßnahme direkt erhöht, sofern es zulässig ist.)	Sicherheit
	→ Unterlassung der technischen Sicherung	Sicherheit

5.1.3 Maßnahmen zu Erhöhung der technischen Verfügbarkeit

Die Ergebnisse der technischen Verfügbarkeit können z. B. als ein Qualitätsmaßstab für die Ereignisbehandlung im Rahmen des technischen Störungsmanagements im Störungsbetrieb (siehe Abbildung 8) angewendet werden. Je schneller die Unregelmäßigkeit im Bahnbetrieb behoben werden kann, desto höher wird die technische Verfügbarkeit.

Die technische Verfügbarkeit im Störungsbereich kann durch das Minimieren der Störungsdauer und/oder das Minimieren des betrieblichen Störungsbereichs erhöht werden. Da die Dauer einer technischen Störung grundsätzlich von der Dauer der Reparatur abhängig ist, kann die technische Verfügbarkeit durch die Reduzierung der Reparaturdauer teils erhöht werden. Um die Reparaturdauer möglichst kurz zu halten, kann z. B. ein Teil der Ereignisbehandlung in der Störung dem betrieblichen Personal überlassen werden. Auch künftig im Fall eines vermuteten IT-Security-Angriffs kann die Behebung der Störung mit passendem Werkzeug und Prozessen direkt von dem betrieblichen Personal ausgeführt werden, ohne die Überprüfung bzw. die Beteiligung des technischen Personals. Allerdings kann die Auslastung des betrieblichen Personals im Störungsbetrieb durch diese zusätzlichen Aufgaben erhöht werden und infolgedessen die Sicherheit des Bahnbetriebs negativ beeinflussen.

Da der Verfügbarkeitsindex von der Größe des Störungsbereichs abhängig ist, kann die technische Verfügbarkeit auch durch das Minimieren des betrieblichen Störungsbereichs erhöht werden. Betrieblich und verfahrenstechnisch gesehen kann dieses Vorhaben z. B. durch das Einrichten einer temporären Räumungsprüfstelle realisiert werden. Durch die temporäre Räumungsprüfstelle soll ermöglicht werden, dass der Bereich der betrieblichen Störung nicht bis zur nächsten Räumungsprüfstelle ausgestreckt werden muss, sondern vorzeitig auf der temporären Räumungsprüfstelle beendet werden kann. Ab dem Standort der temporären Räumungsprüfstelle sollte der Betrieb wieder im technischen gesicherten Regelbetrieb durchgeführt werden können. Durch die temporäre Räumungsprüfstelle kann die Betriebsdichte im Störungsbereich zwar erhöht werden, dies kann jedoch wegen der steigenden Intensität der Handlungen des Fdl eine negative Auswirkung auf die Sicherheit des Bahnbetriebs als Folge haben. Eine Übersicht von den Maßnahmen befindet sich in Tabelle 61.

Tabelle 61: Betriebliche Maßnahmen zur Verbesserung der Verfügbarkeit und deren Konsequenzen

Vorgehensweise	Betriebliche Maßnahmen	Negative Auswirkungen
Minimierung der Störungsdauer	→ Ein Teil der Ereignisbehandlung ist dem betrieblichen Personal überlassen	Sicherheit
Minimierung des betrieblichen Störungsbereichs	→ Einrichten von temporären Räumungsprüfstellen	Sicherheit

5.2 Konzept einer temporären Räumungsprüfstelle

Die Räumungsprüfung ist ein Verfahren zur Sicherung der Abstandhaltung von Zügen auf der freien Strecken und wird heute in Deutschland im Netzbereich der DB Netz AG als Standardverfahren bei Störung des selbsttätigen Streckenblocks angewendet [72]. Nach den betrieblichen Regeln der DB Netz AG ist die Räumungsprüfung nur auf der Räumungsprüfstelle durchzuführen. Eine Räumungsprüfstelle ist die Zugmeldestelle hinter dem gestörten Blockabschnitt, die die Reihenfolge der Züge auf der freien Strecken regelt, z. B. Bahnhöfe [69]. Das bedeutet, dass der Zugfolgeabschnitt auf der freien Strecke während der Räumungsprüfung, sich von der Stelle der Störung bis zum Hauptsignal der nächsten Zugmeldestelle verlängert. Dies hat zur Folge, dass die Zugfolgeabschnitte im Falle einer großräumigen Störung zwischen zwei weit entfernten Zugmeldestellen, wie das Störungsszenario in Kapitel 4.2 zeigt, auf die volle Länge zwischen den beiden Zugmeldestellen verlängert wird. Dadurch wird die Betriebsdichte im Störungsbereich, aufgrund der sehr langen Zugfolgeabschnitte, stark beeinträchtigt. Um die Betriebsdichte zwischen den Zugmeldestellen im Fall solcher großräumigen Störungen erhöhen zu können, wird in dem folgendem Abschnitt diskutiert, wie eine temporäre Räumungsprüfstelle auf einer Strecke mit PZB-Ausrüstung und Ks-Signalen eingerichtet werden kann, sowie welche betrieblichen und technischen Änderungen vorzunehmen sind. Die Diskussion wird sich vorwiegend auf die betriebliche Machbarkeit der temporären Räumungsprüfstelle nach den bestehenden betrieblichen Regeln konzentrieren. Es wird angenommen, dass die technischen Gegebenheiten des Systems das vorgestellte Konzept direkt oder nach einer Anpassung unterstützen können. Insbesondere die individuelle Steuerung des Blocksignals und dessen zugehörigen PZB-Magneten bildet eine Voraussetzung für die Realisierung des vorliegenden Konzepts.

5.2.1 Bereich einer temporären Räumungsprüfstelle

Als Szenario der Diskussion wird, analog zum Störungsbeispiel in Kapitel 4.2, eine freie Strecke mit ortsfestem Ks-Signal und PZB Ausrüstung ausgewählt. Aufgrund einer Störung der Gleisfreimeldeanlagen werden alle Zugfolgeabschnitte der freien Strecke auf der Bedienoberfläche des Fdls als besetzt angezeigt. Alle Blocksignale auf der freien Strecke haben Vor- und Hauptsignalfunktion und zeigen wegen der Störung alle Halt.

Der Bereich einer temporären Räumungsprüfstelle besteht aus zwei Signalabschnitten auf der freien Strecken, dessen Länge den theoretischen Mindestzugfolgeabstand im Regelbetrieb entspricht. Um die Blocksignale einer temporären Räumungsprüfstelle (im Folgenden abgekürzt als TRpst) von den anderen Blocksignalen auf der freien Strecke unterscheiden zu können, sollte es technisch möglich sein die Blocksignale außerhalb der TRpst dunkel zu schalten und zugleich durch ein Kennlicht zu kennzeichnen, wie in Abbildung 32 dargestellt wird. Das hat den Vorteil, dass sich der Tf durch diese Dunkelschaltung besser orientieren kann, ob er sich gerade dem Bereich einer TRpst nähert.

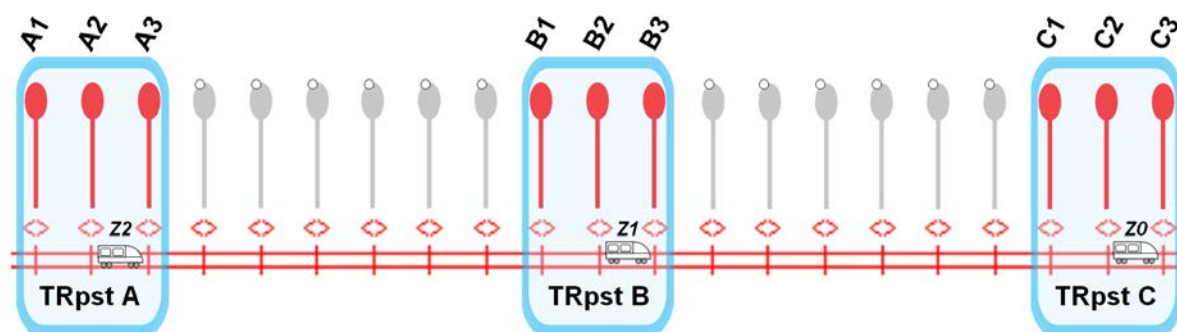


Abbildung 32: Schematische Darstellung von drei temporären Räumungsprüfstellen A, B und C

Eine TRpst darf zu jedem Zeitpunkt maximal von einem Zug belegt werden. Außerdem wird geregelt, dass der Zug in einer TRpst regelmäßig auf dem zweiten Signalabschnitt angehalten wird. Folgen mehrere TRpst auf einer freien Strecke aufeinander, wie die schematische Darstellung in Abbildung 32 zeigt, dann darf ein nachfolgender Zug auf der TRpst A erst losfahren, wenn der vorausfahrende Zug die TRpst B vollständig verlassen hat. D. h., dass ein Zugfolgeabschnitt zwischen den TRpst immer von dem letzten Blocksignal einer TRpst bis zu dem letzten Blocksignal der nächsten TRpst reicht. So z. B. vom Blocksignal A3 bis zum Blocksignal B3 oder vom Blocksignal B3 bis zum Blocksignal C3. Sofern diese Regelung fehlerfrei durchgeführt werden kann, wird bei jeder TRpst lediglich ein Signalabschnitt benötigt. Um das Betriebsrisiko zu reduzieren, wird in dem vorliegenden Konzept auf jeder TRpst ein zusätzlicher Signalabschnitt als Schutzabschnitt geplant. Sollte z. B. der nachfolgende Zug Z2 die TRpst A frühzeitig verlassen haben und anschließend die TRpst B erreicht haben, während der vorausfahrende Zug Z1 sich noch auf der TRpst B zwischen Signalen B2-B3 befinden, dann wird der Z2 aufgrund des Schutzabschnitts B1-B2 nicht direkt mit dem Z1 zur Kollision kommen.

Der technische Hintergrund für das Einrichten des Schutzabschnitts ist das dunkelgeschaltete Hauptsignal mit der Vorsignalfunktion vor dem ersten Blocksignal einer TRpst und somit der fehlende PZB 1000 Hz-Magnet. Aufgrund der Dunkelschaltung wird die Funktion des PZB-Magnets signalgebunden ausgesetzt. Der erste aktive Magnet vor der Einfahrt in die TRpst B, sofern vorhanden, wäre der PZB 500 Hz-Magnet, der ca. 250 m vor dem Blocksignal B1 liegt. Ansonsten kann das Signal B1 mit der höchsten Streckengeschwindigkeit, in diesem Fall 160 km/h, angefahren werden. Auch wenn der 500 Hz-Magnet vor dem Blocksignal B1 vorhanden und aktiv ist, kann Zug 2 mit einer Geschwindigkeit von 160 km/h trotzdem nicht rechtzeitig vor dem Blocksignal B1 anhalten. Ist der Schutzabschnitt nicht vorhanden, dann wird Zug 2 in diesem Fall nach dem Überfahren des haltzeigenden Blocksignals B1 unter Umständen mit Zug 1 bei hoher Geschwindigkeit zusammenstoßen. Das Ergebnis ändert sich, wenn der Schutzabschnitt vorhanden ist. Da das Blocksignal B2 wegen der PZB Überwachung des 500 Hz-Magnets maximal mit 45 km/h angefahren werden darf und der Zug nach dem Vorbeifahren am Blocksignal B2 nach den vorliegenden betrieblichen Regeln gleich in dem zweiten Signalabschnitt anhalten soll, kann im Fall eines Zusammenstoßes eine

Unfallgeschwindigkeit von unter 40 km/h erwartet werden, und somit ein geringes Schadensausmaß.

5.2.2 Räumungsprüfung auf einer temporären Räumungsprüfstelle

Nach den betrieblichen Regeln der Räumungsprüfung müssen die folgenden Prüfbedingungen im Ablauf einer Räumungsprüfung festgestellt werden [69, 72]. Sofern der betreffende Zug dem Fdl bekannt ist gilt:

- Prüfbedingung 1: Hat der betreffende Zug die nächste Zmst erreicht ?,
- Prüfbedingung 2: Wird der betreffende Zug auf der nächsten Zmst durch ein Halt zeigendes Signal gedeckt? und
- Prüfbedingung 3: Ist der betreffenden Zug nach der Ankunft an der nächsten Zmst vollständig?

In der Regel wird heute die Feststellung der Prüfbedingung 1 und 2 vom Fdl anhand der Anzeige seiner Bedienoberfläche realisiert. Sitzt der Fdl in einer weit entfernten Betriebszentrale und kann die Zugvollständigkeit nicht selbst durch die Beobachtung des Zugschlussignals vor Ort feststellen, was heute der Regelfall ist, dann kann der Fdl sich die Prüfbedingung 3 vom Tf oder von einem örtlichen Mitarbeiter bestätigen lassen.

Bei einer Räumungsprüfung auf einer TRpst, wie in dem Störungsszenario in Abbildung 32 dargestellt ist, kann die Feststellung der Prüfbedingung 1 allerdings nicht vom Fdl anhand der Anzeige seiner Bedienoberfläche realisiert werden. Das hat mehrere Gründe. Es kann zum Beispiel sein, dass alle Zugfolgeabschnitte auf der Anzeige aufgrund der Störung als besetzt angezeigt werden und der Fdl nicht sicherstellen kann, in welchem Zugfolgeabschnitt sich der Zug tatsächlich befindet. Ebenfalls kann der Fdl die Zugvollständigkeit nicht selbst feststellen, da er selbst nicht auf der freien Strecke ist und somit den Zugschluss nicht selbst beobachten kann. In diesem Fall muss der Fdl sich die Ankunft und die Zugvollständigkeit des Zuges auf der temporären Räumungsprüfstelle vom Tf bestätigen lassen. Sofern die Prüfbedingung 1 und 3 festgestellt wurden, ist eine Feststellung der Prüfbedingung 2 in dem vorliegenden Störungsszenario nicht notwendig, da alle Signale auf der TRpst aufgrund der Störung Halt zeigen und der Zug auf der TRpst daher stets durch ein haltzeigendes Signal gedeckt wird.

Die Feststellung der Zugvollständigkeit im Störungsbetrieb durch Tf ist bei Zügen mit einer durchgehenden und selbsttätigen Druckluftbremse im Grunde möglich, da im Fall einer Zugtrennung alle Fahrzeuge wegen der Druckabsenkung in der Hauptluftleitung von selbst zum Stehen kommen sollten. Um eine unbemerkte Zugtrennung von Zügen ohne durchgehende und selbsttätige Druckluftbremse zu vermeiden, kann z. B. das Verkehren von solchen Zügen im Störungsbereich verboten werden oder der nachfolgende Zug darf nur auf Sicht durch den Störungsbereich gefahren werden.

Zur Feststellung der Ankunft auf einer TRpst muss der Tf sich nach der Bezeichnung am Blocksignal orientieren. Zu einer besseren Identifizierung für den Tf kann z. B. der zulässige Bereich einer TRpst zwischen zwei Zmst auf bestimmte Blocksignale eingeschränkt werden,

wie das Beispiel in Abbildung 32 zeigt. An dem ausgewählten Blocksignal der TRpst kann z. B. eine besondere Signaltafel zur Kennzeichnung angebracht werden. Um sicherzustellen, dass der Zug sich tatsächlich in dem zweiten Signalabschnitt der TRpst befindet, kann die Signaltafel des letzten Blocksignals einer TRpst mit einer spezifischen Zahlenkombination beschriftet werden. Diese Zahlenkombination ist dem Fdl bekannt, aber nicht dem Tf. Da diese Zahlenkombination nicht als Teil der Fahrerlaubnis übermittelt wurde, kann der Tf diese Zahlenkombination nur direkt von der Signaltafel ablesen. Der Tf muss nach der Ankunft diese Zahlenkombination als Teil der Ankunftsmeldung dem Fdl übermitteln. Dadurch entsteht die Möglichkeit für den Fdl, den Standort des Zuges ohne die technische Anzeige zu überprüfen. Entspricht die von dem Tf übermittelte Zahlenkombination nicht der dem Fdl vorliegenden Zahlenkombination, muss der Fdl davon ausgehen, dass der Tf die entsprechende TRpst noch nicht erreicht oder bereits verlassen hat. In diesem Fall bekommt der nachfolgende Zug auf der vorletzten TRpst solange keine Fahrerlaubnis, bis die Ankunft des vorausfahrenden Zugs auf einer TRpst oder einer Rpst bestätigt wurde.

5.2.3 Betriebsablauf zwischen temporären Räumungsprüfstellen

Anschließend wird in diesem Abschnitt der reguläre Betriebsablauf zwischen TRpst anhand einer Fahrt beispielhaft dargestellt, dies zeigt Abbildung 33. Im Ausgangszustand des Betriebsszenarios steht der Zug 1 nach der Ankunft auf der TRpst A vor dem Blocksignal A3 (Räumungsprüfung bereits abgeschlossen) und wartet auf die Fahrerlaubnis zur Weiterfahrt bis zur TRpst B. Der Fdl erteilt dem Zug 1 die Fahrerlaubnis mit Befehl, dass er am haltzeigenden Signal A3, B1 und B2 vorbeifahren darf und zwischen dem Signal B2 und B3 auf Sicht fahren muss, da der Abschnitt evtl. noch besetzt sein könnte. Anschließend bedient der Tf vom Zug 1 die PZB Befehlstaste zur Vorbeifahrt am haltzeigenden Signal A3. Nachdem der Zug 1 die TRpst A vollständig verlassen hat, muss der Tf dem Fdl eine Verlassensmeldung mitteilen. Diese Verlassensmeldung wird benötigt, da der Fdl wegen der Störung nicht anhand seiner Anzeige feststellen kann, ob der Zug die TRpst tatsächlich verlassen hat. Es kann passieren, dass der Tf die Verlassensmeldung frühzeitig auf der TRpst abgegeben hat, jedoch nicht losgefahren ist. Um das Risiko einer fehlerhaften Verlassensmeldung vom Tf zu reduzieren, wird allen Zügen bereits durch die Fahrerlaubnis befohlen, in dem zweiten Signalabschnitt der TRpst immer auf Sicht zu fahren. Da alle Signale zwischen A3 und B1 ausgeschaltet und durch ein Kennlicht gekennzeichnet wurden, wird die anschließende Zugfahrt zwischen A3 und B1 von der PZB lediglich mit der zulässig höchsten Streckengeschwindigkeit überwacht. Der Tf selbst muss bei der Durchführung der Zugfahrt die streckenseitigen Geschwindigkeitseinschränkungen sowie die Langsamfahrstellen beachten.

Außerdem muss der Tf beachten, dass das erste haltzeigende Blocksignal B1 auf der TRpst B gleich ein Hauptsignal ist. Eine Vorsignalisierung vor dem Blocksignal B1 sowie ein aktiver 1000 Hz-Magnet sind hier nicht gegeben. Daher wurde der Schutzabschnitt auf der TRpst für diesen Fall konzipiert, wie bereits in Kapitel 5.2.1 beschrieben. Der 500 Hz-Magnet vor dem Blocksignal B1 ist aber aktiv. Um nicht beim Vorbeifahren des 500 Hz-Magnets

zwangsgebremst zu werden, muss der Tf die Geschwindigkeit des Zuges gemäß der Überwachungsgeschwindigkeit seiner Zugart bei der Anfahrt reduzieren. Zur Einfahrt in die TRpst B bedient der Tf am Blocksignal B1 die Befehlstaste, um die aktive 2000 Hz-Beeinflussung am Blocksignal B1 zu überbrücken. Mit der Bedienung der Befehlstaste am Blocksignal B1 wird jedoch die aktive 1000 Hz-Beeinflussung aus dem Blocksignal B2 ebenfalls überbrückt. Daher wird der Zug 1 während der Weiterfahrt zwischen dem Blocksignal B1 und B2 nur ab dem 500 Hz-Magnet vor dem Blocksignal B2 durch die Überwachungskurve der PZB überwacht. Zur Vorbeifahrt am haltzeigenden Blocksignal B2 bedient der Tf wieder die Befehlstaste. Der Zug darf bei der Weiterfahrt bis zum Blocksignal B3 nur auf Sicht gefahren werden.

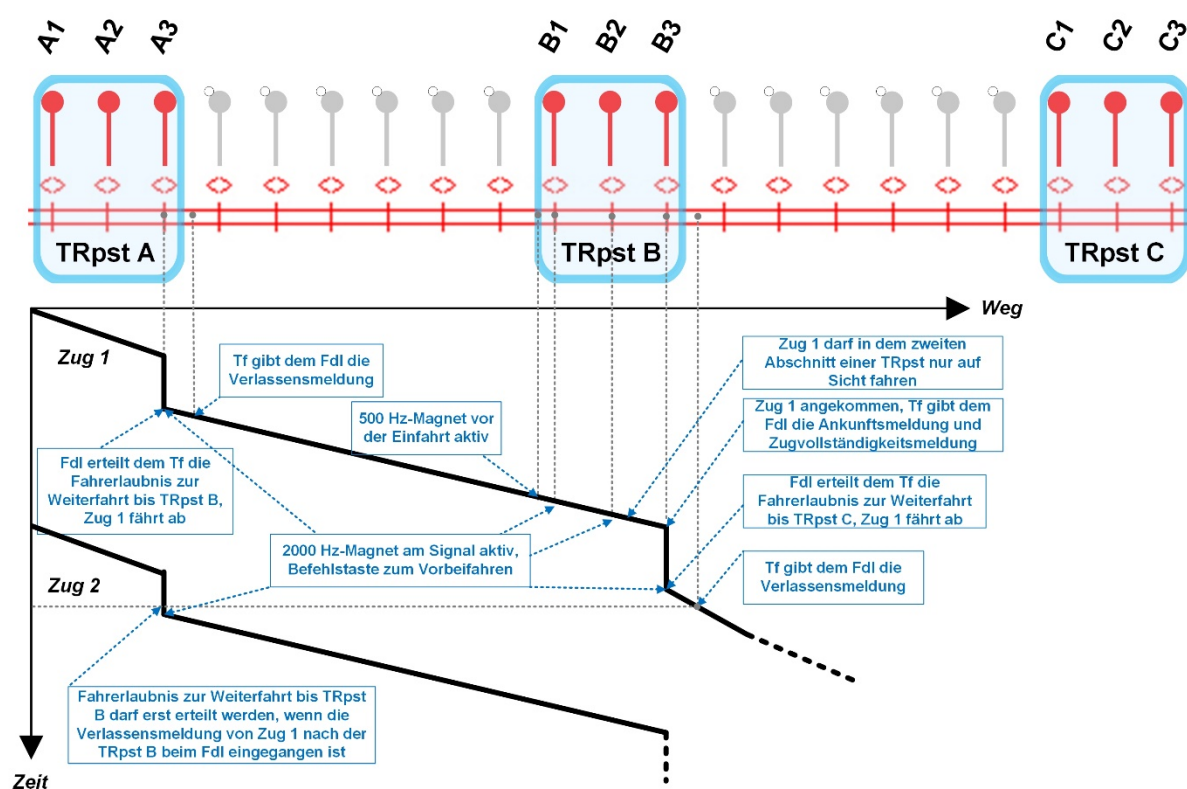


Abbildung 33: Betriebsablauf zwischen den temporären Räumungsprüfstellen

Nach der Ankunft auf der TRpst B bzw. am Blocksignal B3, muss der Tf von Zug 1 dem Fdl eine Ankunfts- und Zugvollständigkeitsmeldung geben. Der Tf muss auch die Vollständigkeit des Zuges 1 sicherstellen und dem Fdl eine Zugvollständigkeitsmeldung übermitteln. Sobald der Fdl die Ankunfts- und Zugvollständigkeitsmeldung vom Tf des Zuges 1 erhalten hat, ist die Räumungsprüfung abgeschlossen. Zu diesem Zeitpunkt wartet Zug 2 bereits auf der TRpst A zur Weiterfahrt. Der Fdl darf dem Zug 2 jedoch noch keine Fahrerlaubnis erteilen, da der Zug 1 die TRpst B noch nicht verlassen hat. Erst wenn der Zug 1 die TRpst B mit der gültigen Fahrerlaubnis verlassen hat und die vorgeschriebene Verlassensmeldung vom Zug 1 beim Fdl eingegangen ist, darf der Fdl dem Zug 2 die Fahrerlaubnis zur Weiterfahrt bis zur TRpst B erteilen.

erteilen. Der beschriebene Betriebsablauf bildet von Beginn des Szenarios bis zu diesem Zeitpunkt einen Regelkreis und wird dann bei den weiteren Zugfahrten wiederholt.

Letztendlich kann die Betriebsdichte zwischen zwei weit entfernten Zugmeldestellen durch das Einrichten einer TRpst zwar erhöht werden, dies kann aber dazu führen, dass die Arbeitsbelastung des Fdl im Störungsbetrieb mit der angestiegenen Betriebsdichte ebenfalls erhöht wird und somit steigt das Betriebsrisiko. Daher ist bei der Gestaltung von Rückfallebenenkonzepten die Wechselwirkung zwischen der Betriebsdichte, der Anzahl der TRpstn und die Auslastung der Menschen durch die Bewertungssystematik zu untersuchen. Anhand dessen wird geprüft, ob das Einrichten der TRpst in dem vorliegenden Störungsbereich und Störungsszenario zweckmäßig ist.

6 Fazit und Ausblick

Durch die zunehmende Anwendung von IT im Eisenbahnwesen bekommt auch die Frage nach ausreichender und gewährleisteter IT-Security einen neuen und wichtigen Stellenwert. Die Bedrohung der IT-Security und ihre Auswirkung auf den Bahnbetrieb sind mittlerweile durch die gesetzlichen Anforderungen und die IT-Security-Vorfälle der Vergangenheit den Fachleuten sehr bewusst. Unabhängig von den getroffenen Vorkehrungen muss davon ausgegangen werden, dass nicht jeder Angriff tatsächlich festgestellt und abgewendet werden kann. Dies bedeutet, dass der Bahnbetrieb nach einem vermuteten oder tatsächlichen IT-Angriff teilweise oder ggf. komplett in der Rückfallebene betrieben werden muss.

Das Rückfallebenenkonzept des Bahnbetriebs hat die Bestrebung, den Bahnbetrieb trotz des Einflusses der vorgegebenen Unregelmäßigkeiten stets mit einer annehmbaren kollektiven Betriebsqualität aus Sicherheit, Leistungsniveau und Verfügbarkeit zu erzielen. Wenn jedoch die Technik nicht mehr oder nur zum Teil funktioniert, dann haben die menschlichen Akteure in der Rückfallebene des Bahnbetriebs die Aufgabe, den Bahnbetrieb in Eigenverantwortung mit oder ohne technische Unterstützung fortzuführen. Das heutige Rückfallebenenkonzept des Bahnbetriebs ist darauf ausgelegt, die bisher anzunehmenden betrieblichen Einschränkungen, in der Regel Safety-Ereignisse und deren Folgen, zu beherrschen. Das sind zumeist kleinräumige und kurzzeitig andauernde Störungen. Wird der Kreis der möglichen Ursachen nun um den IT-Angriff erweitert, dann ist zu erwarten, dass der zukünftige Bahnbetrieb nicht nur häufig in der Rückfallebene durchgeführt werden muss, sondern auch häufiger mit Mehrfachausfällen von Betriebsfunktionen sowie großräumigen und lang andauernden Störungsszenarien konfrontiert sein wird.

Um die Qualitäten des künftigen Störungsbetriebs unter der Bedrohung eines IT-Angriffs systematisch bewerten zu können, wurde im Rahmen dieser Arbeit eine risikoorientierte Systematik zur Bewertung von Rückfallebenenkonzepten entwickelt. Diese Bewertungssystematik ermöglicht die zusammenhängende Berücksichtigung des Störungsszenarios, der systemtechnischen Auslegung, des dynamischen IT-Umfelds, der Charakteristiken des IT-Angriffs sowie die Auslastung der Menschen. Die Anwendung der Bewertungssystematik verfolgt im Wesentlichen das Ziel, die Anwender bei der Gestaltung und der Entscheidungsfindung von Rückfallebenenkonzepten in einer aktuellen dynamischen Betriebslage durch eine schnelle, aber aussagekräftige Risikoschätzung zu unterstützen.

Mit der genannten Zielsetzung begann die Arbeit in Kapitel 2 mit der grundlegenden taxonomischen Differenzierung zwischen Safety und Security sowie deren Bedeutung im Bahnbetrieb. Um die Herausforderung des künftigen Störungsbetriebs unter dem Einfluss eines IT-Angriffs im Vorfeld zu verstehen, wurden als Erstes die Charakteristiken des IT-Angriffs analysiert und deren Unterschiede zu dem bisherigen Safety-Ereignissen in den Punkten Wahrscheinlichkeit, Offenbarung, Ausmaß, Priorität und Dauer herausgestellt. Anschließend wurden die grundlegende Aufgabe, die Bestandteile und die Struktur des Bahnbetriebs sowie

dessen Rückfallebenen aus den funktionalen, gesellschaftlichen und rechtlichen Aspekten eingehend hergeleitet.

Kapitel 3 schließt an mit dem theoretischen Hintergrund der Bewertungssystematik. Beginnend mit der Herleitung der Anforderungen an die Bewertungssystematik, damit sichergestellt werden kann, dass die Variablen und die Aussagen der Bewertungssystematik die wesentlichen Eigenschaften des künftigen Störungsbetriebs angemessenen berücksichtigen. Das Ergebnis einer Ursache- und Wirkungsanalyse hat gezeigt, dass im künftigen Störungsbetrieb tendenziell häufiger komplexe, großräumige und lang andauernde Störungsszenarios zu erwarten sind und dies eine höhere Auslastung der Menschen im Störungsbetrieb verursachen kann. Das System Bahn, als Kritische Infrastruktur, hat aber neben dem sicheren Transport auch die Aufgabe, die Funktionalität und Stabilität der Gesellschaft durch ein angemessenes Leistungsniveau zu gewährleisten. Aufgrund dessen wurde das Konzept Risiko-Budgetierung aus dem Finanzwesen adaptiert und in der vorliegenden Arbeit zur proaktiven Steuerung von Betriebsrisiko sowie zur Erhöhung der Gestaltungsfreiheit von Rückfallebenenkonzepten vorgestellt. Die risikobasierte Bewertungssystematik zur Ermittlung des Betriebsrisikos besteht nach dem Risikomodell aus sieben Strukturteilen. Dazu gehören das Betriebsszenario, das Funktionsmodell, das Versagenspotenzial, die Anzahl der Versagen, das IT-Manipulationspotenzial, der Reduktionsfaktor und das Schadensausmaß. Um die Betriebsqualitäten von unterschiedlichen Rückfallebenenkonzepten intuitiv vergleichen zu können, werden die maßgeblichen Ergebnisse der Bewertung als Index dargestellt. Der Risikoindex zeigt die Sicherheit des Rückfallebenenkonzepts, der Leistungsindex bildet das Leistungsniveau des Rückfallebenenkonzepts ab und der Verfügbarkeitsindex stellt den Stand der technischen Verfügbarkeit dar.

Die Anwendung der Bewertungssystematik wurde anschließend in Kapitel 4 anhand einer großräumigen und lang andauernden Störung der Gleisfreimeldeanlage auf der freien Strecke zwischen zwei Zugmeldestellen demonstriert. Ausgehend von der Festlegung der grundlegenden Parameter des Betrachtungsbereichs und der Definition des Störungsszenarios wurden insgesamt zehn Basisvarianten und vier kombinierte Varianten von Rückfallebenenkonzepten für das vorliegende Störungsszenario konzipiert und anhand der Bewertungssystematik untersucht. Das Ergebnis des Variantenvergleichs hat gezeigt, dass der Bahnbetrieb unter der heutigen verfahrenstechnischen Einschränkung bzw. des heutigen Rückfallebenenkonzepts bei einer derartigen Störung, deren IT-Manipulationspotenzials sehr gering ist, zwar auf Dauer durchgeführt werden kann, jedoch nicht mehr leistungsfähig ist.

Abschließend wurde in Kapitel 5 die Optimierungsmöglichkeit der Betriebsqualitäten in Bezug auf die Anwendung der Bewertungssystematik diskutiert. Ebenfalls wird das Konzept einer temporären Räumungsprüfstelle auf der freien Strecke, mit der die Betriebsdichte einer Strecke im Fall einer großräumigen Störung ohne die Änderung der Beförderungsgeschwindigkeit erhöht werden kann, eingehend vorgestellt und analysiert. Das Ergebnis der Untersuchung zeigte, dass das Konzept nach den bestehenden Regelwerken betrieblich realisierbar ist, insofern die zugehörigen technischen Systeme es funktionell unterstützen.

Insgesamt ergibt sich, als Schlussfolgerung dieser Arbeit, dass die vorgestellte Bewertungssystematik ihren Anwendern ermöglicht, künftig bei der Gestaltung von Rückfallebenenkonzepten neben dem Störungsszenario, auch das dynamische IT-Umfeld, die Charakteristiken des IT-Angriffs, die menschliche Auslastung und die systemtechnische Auslegung zusammenhängend zu berücksichtigen. Die Bewertungssystematik unterstützt den Anwender bei der Gestaltung und Entscheidungsfindung von Rückfallebenenkonzepten mit einer schnellen, aber wissenschaftlichen fundierten Qualitätseinschätzung. Sollte der künftige Bahnbetrieb unter der Bedrohung eines IT-Angriffs tatsächlich häufig in den komplexen, großräumigen und lang andauernden Störungsszenarios durchgeführt werden müssen, dann lassen sich eine risikoorientierte Gestaltung von Rückfallebenenkonzepten und eine proaktive Steuerung von Betriebsrisiken durch die Anwendung dieser Bewertungssystematik realisieren.

Als Ausblick für zukünftige Forschung und die Praxisanwendung der Bewertungssystematik steht nach wie vor die Herausforderung, wie das menschliche Versagenspotenzial in den Rückfallebenen genau einzuschätzen ist, aus. Da die Menschen im Vergleich zu den technischen Systemen in der Regel ein deutlich höheres Versagenspotenzial haben, werden die Lösungsräume der Rückfallebenenkonzepten aufgrund des risikoorientierten Bewertungsansatzes von dem Versagenspotenzial der Menschen wesentlich beeinflusst. Im Angesicht der zunehmenden Automatisierung, Digitalisierung, Virtualisierung und der daraus resultierenden Änderung des menschlichen Arbeitsverhaltens im Bahnbetrieb muss hinterfragt werden, ob und wie lange die heutigen Kenntnisse über das menschliche Versagenspotenzial im Bahnbetrieb noch gelten werden.

Trotz allem, stellt das IT-Manipulationspotenzial im Bahnbetrieb mit seiner Unberechenbarkeit den größten Unsicherheitsfaktor bei der Einschätzung des Betriebsrisikos dar. Da das Thema IT-Security zum jetzigen Zeitpunkt im Bahnbereich noch recht neu ist und es bisher keine umfassenden Kenntnisse über das tatsächliche Geschehen auf einer komplett digitalisierten Bahninfrastruktur gibt, muss der Einfluss des IT-Angriffs auf das Betriebsrisiko künftig im Laufe der technischen Migration noch weiter verfolgt und genau untersucht werden. Letzten Endes besteht künftig weiterhin die Herausforderung einer gesellschaftlichen Debatte über die Qualitätsanforderung der Bahn als Kritische Infrastruktur, in der auch das Thema Risiko-Budgetierung einzuschließen ist. Wird der künftige Bahnbetrieb unter der Bedrohung des IT-Angriffs häufig mit der großräumigen und lang andauernden Störung konfrontiert, dann ist eine genaue Abwägung zwischen dem Funktionieren und dem Risiko des Bahnbetriebs nach der gesellschaftlichen Wertvorstellung unerlässlich.

Abkürzungsverzeichnis

AEG	Allgemeines Eisenbahngesetz
BZ	Betriebszentrale
COTS	Commercial off-the-shelf System
CSM	Common Safety Method
DB	Deutsche Bahn
EBO	Eisenbahn-Bau- und Betriebsordnung
EIU	Eisenbahninfrastrukturunternehmen
EVU	Eisenbahnverkehrsunternehmen
Fa.	Funktionsablauf
Fdl	Fahrdienstleiter
GZ	Güterzug
Ha.	Handlungsablauf
HVZ	Hauptverkehrszeit
IT	Information Technology
IZB	Infrastrukturzustands- und Entwicklungsbericht
KRITIS	Kritische Infrastruktur
LI	Leistungsindex
LST	Leit- und Sicherungstechnik
NVZ	Normalverkehrszeit
NV	Nachtverkehrszeit
RAC-TS	Risikogrenzwert für technische Systeme
RI	Risikoindex
Rpst	Räumungsprüfstelle
RSM	Risk Score Matrix
RZ	Reisezug
SPFV	Schienenpersonennahverkehr
SPNV	Schienenpersonenfernverkehr
SGV	Schienengüterverkehr
SVZ	Schwachverkehrszeit
Tf	Triebfahrzeugführer
Trkm	Trassenkilometer
TRpst	Temporäre Räumungsprüfstelle
Zmst	Zugmeldestelle

Literaturverzeichnis

- [1] Huang, Po-Chi ; Milius, Birgit: IT-Security für einen sicheren Bahnbetrieb, In: *Deine Bahn* (2016), Heft 2, S. 13–16
- [2] Kriaa, Siwar ; Pietre-Cambacedes, Ludovic ; Bouissou, Marc ; Halgand, Yoran: A survey of approaches combining safety and security for industrial control systems, In: *Reliability Engineering & System Safety* 139 (2015), S. 156–178
- [3] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.): Leitfaden Cyber-Sicherheits-Check, Bonn, Februar 2014
- [4] Wikipedia: *Stuxnet*, <http://de.wikipedia.org/wiki/Stuxnet>. - abgerufen am 2019-11-01
- [5] CBS News: *Virus Disrupts Train Signals*, <https://www.cbsnews.com/news/virus-disrupts-train-signals/>. - abgerufen am 2019-11-01
- [6] The Register: *Polish teen derails tram after hacking train Security network*, http://www.theregister.co.uk/2008/01/11/tram_hack/. - abgerufen am 2019-11-01
- [7] Nextgov: *Hackers manipulated Railway Computers, TSA Memo says.*,
- [8] Heise Online: *Ransomware WannaCry befällt Rechner der Deutschen Bahn*, <https://www.heise.de/newsticker/meldung/Ransomware-WannaCry-befaeilt-Rechner-der-Deutschen-Bahn-3713426.html?view=print>. - abgerufen am 2019-11-01
- [9] Zeit Online: *Bundesamt warnt vor neuer Qualität der Internetkriminalität*, <https://www.zeit.de/digital/internet/2018-10/hackerangriffe-gefaehrungslage-bundesamt-sicherheit-informationstechnik>. - abgerufen am 2019-11-01
- [10] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Bonn: Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31, 24. Juli 2015
- [11] Bundesministerium des Innern: *Schutz Kritischer Infrastrukturen – Basisschutzkonzept*, Berlin, 2005
- [12] Bundesministerium des Innern: *Empfehlungen zur Sicherstellung des Zusammenwirkens zwischen staatlichen Ebenen des Krisenmanagements und den Betreibern Kritischer Infrastrukturen*, Berlin, 2010
- [13] Bundesministerium des Innern: *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden*, Berlin, 2011
- [14] DIN EN ISO 22301 Sicherheit und Schutz des Gemeinwesens – Business Continuity Management System – Anforderungen, Dezember 2014
- [15] FprEN ISO 22313 Sicherheit und Schutz des Gemeinwesens – Aufrechterhaltung der Betriebsfähigkeit – Leitlinie, Juli 2014
- [16] ISO/IEC 27031 Information technology – Security techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity, März 2011
- [17] DB Netz AG: Richtlinie 420.1000: Störungsmanagement Betriebszentralen - gültig ab 15.12.2013
- [18] DUDEN: *Sicherheit*, <https://www.duden.de/rechtschreibung/Sicherheit#Bedeutung1>. - abgerufen am 2019-11-01
- [19] Aven, Terje: On the link between risk and exposure, In: *Reliability Engineering & System Safety* 106 (2012), S. 191–199
- [20] Durchführungsverordnung (EU) Nr. 402/2013: Gemeinsame Sicherheitsmethode für

-
- die Evaluierung und Bewertung von Risiken, 2013
- [21] DIN EN 50129 Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsbezogene elektronische Systeme für Signaltechnik, Juni 2019
 - [22] DIN EN 50126-2 Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 2: Systembezogene Sicherheitsmethodik, Oktober 2018
 - [23] Line, Maria B. ; Nordland, Odd ; Røstad, Lillian ; Tøndel, Inger Anne: SAFETY VS. SECURITY?, In: *Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management*, 2006
 - [24] Braband, Jens: Spannungsfeld Safety und Security: gestern, heute, morgen, In: *Deine Bahn* 03 (2018), S. 6–11
 - [25] Aven, Terje: What is safety science?, In: *Safety Science* 67 (2014), S. 15–20
 - [26] Deine Bahn: Sicherheitsexperten auf den neuesten Stand gebracht, In: *Deine Bahn* (2015), Heft 1, S. 52–56
 - [27] DIN EN 50126-1 Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 1: Generischer RAMS-Prozess, Oktober 2018
 - [28] SRA: *Society for risk analysis glossary*, 2015
 - [29] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-1: Managementsysteme für Informationssicherheit, 2017
 - [30] DIN VDE V 0831-102 Elektrische Bahn-Signalanlagen – Teil 102: Schutzprofil für technische Funktionen in der Eisenbahnsignaltechnik, Dezember 2013
 - [31] ISO/IEC 27000:2018 - Information security management systems — Overview and vocabulary
 - [32] Maal, M. ; Brattekkås, K. ; Nystuen, K. O. ; Windvik, R.: How to assess future security threats to critical infrastructure systems? Lessons learnt and best practices from a security risk assessment of the ERTMS in Norway, In: *Safety and Reliability – Theory and Applications, 27th European Safety and Reliability Conference*, London: CRC Press Taylor & Francis Group, 2017, S. 1139–1146
 - [33] Hartong, Mark ; Goel, Rajni ; Wijesekera, Duminda: Securing Positive Train Control Systems, In: Goetz, E. ; Sheno, S. (Hrsg.): *Critical Infrastructure Protection, IFIP International Federation for Information Processing*. 253, Boston, MA: Springer US, 2008, S. 57–72
 - [34] Trustwave: *2017 Trustwave global Security Report*, 2017
 - [35] Fireeye: *M-Trends 2017*, 2017
 - [36] DERWESTEN: *Bahn-Chaos im Ruhrgebiet bis weit in die Nacht*, <https://www.derwesten.de/staedte/duisburg/bahn-verspaetung-sperrung-bekennerschreiben-id215401601.html>. - abgerufen am 2019-11-01
 - [37] Westfalenpost: *Sabotage an Bahnstrecke in NRW - Reparatur dauert länger*, <https://www.wp.de/region/rhein-und-ruhr/sabotage-akt-gegen-bahn-in-nrw-strecke-wieder-freigegeben-id215409937.html>. - abgerufen am 2019-11-01
 - [38] Bosse, Gunnar: *Grundlagen für ein generisches Referenzsystem für die Betriebsverfahren spurgeführter Verkehrssysteme*, Technische Universität Carolo-Wilhelmina zu Braunschweig, Dissertation, 2011
-

-
- [39] Pachl, Jörn: Die Bedeutung betrieblicher Regelwerke für die Leit- und Sicherungstechnik, In: *Signal + Draht* (2008), Heft 12, S. 32–38
- [40] Maschek, Ulrich: *Sicherung des Schienenverkehrs*: Springer Vieweg, 2018
- [41] Richtlinie (EU) 2016/797: Interoperabilität des Eisenbahnsystems in der Europäischen Union
- [42] Fenner, Wolfgang ; Peter, Naumann ; Trinckauf, Jochen: *Bahnsicherungstechnik*, Erlangen: Publicis Publishing, 2004
- [43] Gesetz zur Regionalisierung des öffentlichen Personennahverkehrs, 2016
- [44] Allianz pro Schiene: *Hintergrund: Regionalisierung des Schienennahverkehrs*, <https://www.allianz-pro-schiene.de/themen/personenverkehr/regionalverkehr/hintergrund-regionalisierung-des-schienennahverkehrs/>. - abgerufen am 2019-11-01
- [45] DB Netz AG: *Infrastrukturzustands- und -entwicklungsbericht 2017*, 2018
- [46] Deutsche Bahn AG: *Daten & Fakten 2017*, 2018
- [47] VDV: *VDV Jahresbericht 2017/2018*, 2018
- [48] Richtlinie 2008/114/EG: Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern
- [49] Aktiengesetz, 2015
- [50] Richtlinie (EU) 2016/798: Eisenbahnsicherheit
- [51] Allianz pro Schiene: *Die Bahn ist das sicherste Verkehrsmittel*, <https://www.allianz-pro-schiene.de/themen/sicherheit/daten-fakten/>. - abgerufen am 2019-11-01
- [52] VCÖ: *Hohe Effizienz beim Öffentlichen Verkehr*, [https://www.vcoe.at/files/vcoe/uploads/Infografiken/Oeffentlicher Verkehr/VCÖ-Grafik Hohe Effizienz beim ÖV.png](https://www.vcoe.at/files/vcoe/uploads/Infografiken/Oeffentlicher%20Verkehr/VC%C3%96-Grafik%20Hohe%20Effizienz%20beim%20%C3%96V.png). - abgerufen am 2019-11-01
- [53] VCÖ: *Mit der U-Bahn werden 25 Mal so viele Personen pro Stunde befördert wie mit dem Pkw*, [https://www.vcoe.at/files/vcoe/uploads/Infografiken/Oeffentlicher Verkehr/161116_VCOE_Einzelgrafiken-02%28groß%29.jpg](https://www.vcoe.at/files/vcoe/uploads/Infografiken/Oeffentlicher%20Verkehr/161116_VCOE_Einzelgrafiken-02%28gro%C3%9F%29.jpg). - abgerufen am 2019-11-01
- [54] Asian Development Bank: *Changing Course in Urban Transport*, 2011
- [55] Allianz pro Schiene: *Überblick: Wie der Güterzug länger werden kann*, <https://www.allianz-pro-schiene.de/themen/aktuell/740-meter-gueterzug/#>. - abgerufen am 2019-11-01
- [56] Breimeier, Rudolf: Neue Autobahnen oder Eisenbahnen für den wachsenden Güterverkehr in Deutschland. Teil 2: Auf dem Weg zu einer marktfähigen Güterbahn in Deutschland?, In: *Eisenbahn-Revue International* 8–9 (2014), S. 426–430
- [57] California High-Speed Rail Authority: *Service Planning Methodology*, 2018
- [58] High Speed Two Ltd: *Signalling Headways and Maximum Operational Capacity on High Speed Two London to West Midlands Route*, 2011
- [59] Castells, Ramon Malla: Automated metro operation: greater capacity and safer, more efficient transport, In: *Public Transport International* 11/12 (2011), S. 15–21
- [60] CBTC tackles Copenhagen's growth and aims for 25% headway reduction, <https://www.smartrailworld.com/cbtc-tackles-copenhagens-growth-and-aims-for-25-headway-reduction>. - abgerufen am 2019-11-01
-

-
- [61] Transport for London: *London Underground World Class Capacity sub Programme Review*, 2017
- [62] Umwelt Bundesamt: *Schienennetz 2025/2030 - Ausbaukonzeption für einen leistungsfähigen Schienengüterverkehr in Deutschland*, 2010
- [63] Richtlinie 2012/34/EU: Schaffung eines einheitlichen europäischen Eisenbahnraums
- [64] Naumann, Peter ; Pachl, Jörn: *Leit- und Sicherungstechnik im Bahnbetrieb*. 2. Aufl., Hamburg: Tetzlaff Verlag, 2004
- [65] Allgemeines Eisenbahngesetz (AEG), 2015
- [66] Jacobs, Jürgen: *Rechnerunterstützte Konfliktermittlung und Entscheidungsunterstützung bei der Disposition des Zuglaufs*, Rheinisch-Westfälischen Technischen Hochschule Aachen, Dissertation, 2003
- [67] DB Netz AG: Richtlinie 420: Betriebszentrale DB Netz AG - gültig ab 15.12.2013
- [68] Eisenbahn-Bau- und Betriebsordnung (EBO), 2019
- [69] DB Netz AG: Fahrdienstvorschrift Richtlinien 408.01-06 und 408.48, gültig ab 10.12.2017
- [70] Pachl, Jörn: *Besonderheiten ausländischer Eisenbahnbetriebsverfahren*, Wiesbaden: Springer Vieweg, 2016
- [71] Pachl, Jörn: Übertragbarkeit US-amerikanischer Betriebsverfahren auf europäische Verhältnisse, In: *ETR 50* (2001), Heft 7/8, S. 452–462
- [72] Pachl, Jörn: *Systemtechnik des Schienenverkehrs – Bahnbetrieb planen, steuern und sichern*. 9. Aufl., Wiesbaden: Springer Vieweg, 2018
- [73] Pachl, Jörn: Betriebssicherheitliche Regelwerke im internationalen Vergleich, In: *Eisenbahningenieur* (2012), Heft 02, S. 48–52
- [74] Huang, Po-Chi: A multipurpose generic framework for developing systematic railway operational rules, In: *Journal of Polish Safety and Reliability Association, Proceedings of Summer Safety and Reliability Seminars*. 9, 2018, S. 31–38
- [75] Milius, Birgit ; Huang, Po-Chi: Sichere Rückfallebenen in Zeiten der Rail-IT-Automation, In: *Der Eisenbahningenieur* 11 (2017), S. 36–39
- [76] Bainbridge, Lianne: Ironies of automation, In: *Automatica* (1983)
- [77] Hinzen, Albrecht: *Der Einfluss des menschlichen Fehlers auf die Sicherheit der Eisenbahn*, Rheinisch-Westfälische Technische Hochschule Aachen, Dissertation, 1993
- [78] Kücükaya, Alper: *Bewertung der menschlichen Zuverlässigkeit in der semi-quantitativen Risk Score Matrix nach DIN VDE V 0831-103*, Technische Universität Carolo-Wilhelmina zu Braunschweig, Masterarbeit, 2018
- [79] Lindner, Tobias: *Entwicklung einer Methodik zur Erfassung des Situationsbewusstseins an Arbeitsplätzen in elektronischen Stellwerken und Betriebszentralen*, Technische Universität Carolo-Wilhelmina zu Braunschweig, 2015
- [80] Hammerl, Malte: *Analyse der menschlichen Einflussfaktoren und Zuverlässigkeit im Eisenbahnverkehr*, Technische Universität Carolo-Wilhelmina zu Braunschweig, Dissertation, 2011
- [81] Deutsche Bahn AG: *Bemessung der Arbeitsplätze*, 1995
- [82] *Betriebssteuerung RB Süd: Ein Blick in die Betriebszentrale München*, <https://bahnblogstelle.net/2015/10/29/betriebssteuerung-rb-sued-ein-blick-in-die->
-

- betriebszentrale-muenchen/. - abgerufen am 2019-11-01
- [83] Gerrits, Lasse ; Schipper, Danny: *Internationale Vergleichsstudie zum Eisenbahnstörungsmanagement*, Bamberg: OPUS, 2018
- [84] Durchführungsverordnung (EU) 2015/1136: zur Änderung der Durchführungsverordnung (EU) Nr. 402/2013 über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken, 2015
- [85] DIN: DIN VDE V 0831-103: Ermittlung von Sicherheitsanforderungen an technische Funktionen in der Eisenbahnsignaltechnik, November 2014
- [86] DIN: DIN VDE V 0831-101: Semiquantitative Verfahren zur Risikoanalyse technischer Funktionen in der Eisenbahnsignaltechnik, März 2011
- [87] Bepperling, Sonja-Lara: *Validierung eines semi-quantitativen Ansatzes zur Risikobeurteilung in der Eisenbahntechnik*, Technische Universität Carolo-Wilhelmina zu Braunschweig, Dissertation, 2008
- [88] Statistisches Bundesamt: *Verkehrsunfälle Fachserie 8 Reihe 7 - 2017*, 2018
- [89] Braband, Jens: *Risikoanalysen in der Eisenbahn-Automatisierung*, Hamburg: Eurailpress, 2005
- [90] Höppner, Silko: *Generische Beschreibung von Eisenbahnbetriebsprozessen*, ETH Zürich, 2014
- [91] Milius, Birgit: *Konstruktion eines semi-qualitativen Risikographen für das Eisenbahnwesen*, Technische Universität Carolo-Wilhelmina zu Braunschweig, 2009
- [92] Statistisches Bundesamt: *Betriebsdaten des Schienenverkehrs Fachserie 8 Reihe 2.1 - 2011*, 2012
- [93] Statistisches Bundesamt: *Betriebsdaten des Schienenverkehrs Fachserie 8 Reihe 2.1 - 2017*, 2018
- [94] Bepperling, Sonja-Lara: Eine generische Risikobeurteilung für den Zugleitbetrieb, In: *Signal + Draht* 3 (2010), S. 19–23
- [95] DB Netz AG: Richtlinie 413.0301 - Streckenstandards, 2002
- [96] Schäbe, Hendrik: Definition of Safety Integrity Levels and the Influence of Assumptions, Methods and Principles Used, In: C. Spitzer et al. (Hrsg.): *Probabilistic Safety Assessment and Management*: Springer-Verlag London, 2004, S. 1020–1025
- [97] Vaurio, J.K.: Safety-related decision making at a nuclear power plant, In: *Nuclear Engineering and Design* (1998), Heft 185, S. 335–345
- [98] Jespen, Torben: *Risk Assessments and Safe Machinery*: Springer, 2016
- [99] Joksimovic, V. ; Solomon, K. A.: Quantitative Safety Goals Through More Adequate Risk Management and Risk Assessment, In: *Reliability Engineering* (1983), Heft 4, S. 65–84
- [100] Finanztreff: *Börsenlexikon*, www.finanztreff.de/wissen/boersenlexikon/tracking-error/5367. - abgerufen am 2019-11-01
- [101] PPCmetrics AG: *Finanzlexikon*, <https://www.ppcmetrics.ch/de/publikationen/finanzlexikon/risk-budgeting/>. - abgerufen am 2019-11-01
- [102] Lefer, Luc: *Do you say risk budget?*, <https://wealthmanagement.bnpparibas/en/expert-voices/did-you-say-risk-budget.html#>. - abgerufen am 2019-11-01

-
- [103] Meketa Investment Group: *Risk Budgeting*
- [104] Rahl, L. (Hrsg.): *Risk Budgeting: A New Approach to Investing*, London, 2000
- [105] DB Netz AG: *Infrastrukturzustands- und -entwicklungsbericht 2012*, 2013
- [106] Leistungs- und Finanzierungsvereinbarung II zwischen der Bundesrepublik Deutschland und der DB Netz AG, der DB Station&Service AG, der DB Energie GmbH sowie der Deutschen Bahn AG, 2015
- [107] DB Netz AG: *Infrastrukturzustands- und -entwicklungsbericht 2018*, 2019
- [108] CENELEC: DIN EN 61025:2006 Fehlzustandsbaumanalyse, 2006
- [109] DIN: DIN EN 62267 Automatischer städtischer schienengebundener Personennahverkehr, 2010
- [110] Brünenberg, Dirk ; Enders, Dirk H ; Gullasch, Jennifer ; Hartmann, Jens ; Six, Jürgen: Risikoanalyse FFB - Ursachen- und Folgenanalyse anhand von Beispielen, In: *Signal + Draht* 10 (2001), S. 18–25
- [111] Arbeitszeitgesetz, 2016
- [112] DIN VDE V 0831-104 Elektrische Bahn-Signalanlagen – Teil 104: Leitfaden für die IT-Sicherheit auf Grundlage 62443, Oktober 2015
- [113] ISO/IEC 27005:2018 Information security risk management
- [114] IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels
- [115] prEN 62443-3-2: 2018 (Entwurf) Sicherheit für industrielle Automatisierungssysteme - Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung
- [116] KRITIS Glossar,
https://www.kritis.bund.de/SubSites/Kritis/DE/Servicefunktionen/Glossar/glossar_node.html. - abgerufen am 2019-11-01
- [117] NIST: *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*, 2018
- [118] U.S. Department of Energy (DOE) (Hrsg.): *Cybersecurity Capability Maturity Model Version 1.1*, 2014
- [119] CCRA: *Common Criteria (Version 3.1, Release 5)*,
<https://www.commoncriteriaportal.org/cc/>. - abgerufen am 2019-11-01
- [120] Ross, Sebastian: *Strategische Infrastrukturplanung im Schienenverkehr*: Deutscher Universitäts-Verlag, 2001
- [121] *Züge im Fernverkehr*,
https://www.bahn.de/p/view/service/zug/fahrzeuge/zugtypen.shtml?dbkanal_007=L01_S01_D001_KIN_-rs-zug_NAVIGATION-fahrzeuge_LZ01. - abgerufen am 2019-11-01
- [122] PWC GmbH (Hrsg.): *Studie zur Gestaltung und Entwicklung der Eisenbahninfrastrukturpreise in Europa*, 2018
- [123] Eisenbahn-Bundesamt: Allgemeinverfügung zum Melden von gefährlichen Ereignissen im Eisenbahnbetrieb, 2010
- [124] *ICE-Unfall von Eschede*, https://de.wikipedia.org/wiki/ICE-Unfall_von_Eschede. - abgerufen am 2019-11-01
- [125] *Santiago de Compostela derailment*,
-

-
- https://en.wikipedia.org/wiki/Santiago_de_Compostela_derailment. - abgerufen am 2019-11-01
- [126] *Eisenbahnunfall von Xinma*,
https://de.wikipedia.org/wiki/Eisenbahnunfall_von_Xinma. - abgerufen am 2019-11-01
- [127] *Southall rail crash*, https://en.wikipedia.org/wiki/Southall_rail_crash. - abgerufen am 2019-11-01
- [128] *Eisenbahnunfall von Ladbroke Grove*,
https://de.wikipedia.org/wiki/Eisenbahnunfall_von_Ladbroke_Grove. - abgerufen am 2019-11-01
- [129] *Eisenbahnunfall von Bad Aibling*,
https://de.wikipedia.org/wiki/Eisenbahnunfall_von_Bad_Aibling. - abgerufen am 2019-11-01
- [130] Fendrich, Lothar ; Wolfgang, Fengler (Hrsg.): *Handbuch Eisenbahninfrastruktur*, Berlin, Heidelberg: Springer Vieweg, 2013
- [131] Schnieder, Lars: *Betriebsplanung im öffentlichen Personennahverkehr*, Berlin: Springer Vieweg, 2018
- [132] BMVI: *Machbarkeitsstudie zur Prüfung eines Deutschland-Takts im Schienenverkehr*, 2015
- [133] DB Netz AG: *Anlage 6.1 zu den Schienennetz-Benutzungsbedingungen der DB Netz AG 2019*, 2018
- [134] Innoverse GmbH: *Entwicklungsstrategie für den Schienenpersonennahverkehr (SPNV) in Berlin und Brandenburg*, 2017
- [135] ÖPNV-Zukunftskommission NRW: *Zukunft des ÖPNV in NRW Weichenstellung für 2020/2050*, 2013
- [136] Europäischer Rechnungshof: *Der Schienengüterverkehr in der EU: noch nicht auf dem richtigen Kurs*, 2016
- [137] Bühler, Georg: *Verkehrsmittelwahl im Güterverkehr*, Albert-Ludwigs-Universität Freiburg, Dissertation, 2005
- [138] Huang, Po-Chi: Risiko der betrieblichen Rückfallebene im digitalen Bahnbetrieb, In: *Der Eisenbahningenieur* (2019), Heft 8, S. 54–56
- [139] Huang, Po-Chi: Risikobasierter Ansatz zur Bewertung von betrieblichen Rückfallebenen, In: *ZEVrail* (2020), Heft 1–2, S. 26–31
- [140] Theeg, G. ; Vlasenko, S. (Hrsg.): *Railway Signalling & Interlocking*. Eurail pre. Aufl., 2017
-

Anhang A: Mittlere Beförderungsgeschwindigkeit

Einschätzung der mittleren Beförderungsgeschwindigkeit

- SPFV: 140 km/h (Angenommene Geschwindigkeit in der vorliegenden Arbeit)

Quelle	Text	Geschwindigkeit
[132]	Bei Betrachtung der Schnellfahrstrecken ergeben sich durchschnittliche Reisegeschwindigkeiten bis 170 km/h, im Fernverkehr, der Bestands- und Neubaustrecken nutzt, sind dies 120-150 km/h.	120 - 150 km/h
[133]	Neben diesen beiden Geschwindigkeitsbereichen (unter 100 km/h und über 160 km/h) weist das Geschwindigkeitsprofil des SPFV vorwiegend Verkehre mit einer Durchschnittsgeschwindigkeit zwischen 100 und 160 km/h auf.	100 - 160 km/h

- SPNV: 70 km/h (Angenommene Geschwindigkeit in der vorliegenden Arbeit)

Quelle	Text	Geschwindigkeit
[134]	(Mittelwert der Reisegeschwindigkeit aus aller SPNV Verbindungen von Brandenburger Städte und Gemeinden über 10.000 Einwohner nach Berlin im Fahrplan Jahr 2016)	70 km/h
[135]	In NRW beträgt die mittlere Luftliniengeschwindigkeit auf dem Schienennetz 30,29 km/h (Verbindungsgüte), damit ist sie weitaus geringer als der Bundesdurchschnitt (70,58 km/h). Der zentrale Indikator für den Beitrag der Verkehrsträger zur Qualität der Raumüberwindung ist die Verbindungsgüte. Sie bildet die durchschnittliche Reisegeschwindigkeit – gemessen als mittlere Luftliniengeschwindigkeit, die als das Verhältnis von Luftlinienentfernung und realer Fahrtzeit definiert ist – zwischen allen Unterregionen (Kreise und kreisfreien Städte) einer Oberregion (Bundesländer, Staaten oder Staatenverbünde) ab. Als Grundlage für die Bestimmung der Reisezeiten dienen die Fahrpläne des Schienenpersonenverkehrs.	70 km/h
[122]	(Durchschnittsgeschwindigkeit des Musterzugs im SPNV-Ballungsraum zur Studie der Gestaltung und Entwicklung der Eisenbahninfrastrukturpreise im Auftrag der Deutschen Bahn AG)	60 km/h

- SGV: 50 km/h (Angenommene Geschwindigkeit in der vorliegenden Arbeit)

Quelle	Text	Geschwindigkeit
[136]	In den Schienengüterverkehrskorridoren ist die Durchschnittsgeschwindigkeit von Zügen jedoch mit der von Lkw in etwa vergleichbar.	50 km/h
[137]	Transporte mit deutschen Lkw werden laut Angaben aus der empirischen Erhebung mit einer Durchschnittsgeschwindigkeit von 50,06 km/h betrieben	50 km/h
[77]	(Mittelwert aus der Anlage 9)	45 km/h

Anhang B: Unfallklasse nach VDE V 0831-103 [85]

Unfallklasse	Maßgebendes Schadensausmaß	Typische Ereignisarten
A	Kein Personenschaden	Aufprall einer Rangierfahrt auf Gleissperre
		Aufprall einer Rangierfahrt auf Gegenstand
		Unzeitige Zwangsbremmung
B	Ein Leichtverletzter	Aufprall eines Reisezuges auf Gegenstand bei niedriger Geschwindigkeit
		Aufprall eines Güterzuges auf Gegenstand
		Entgleisung einer Rangierfahrt
		Zusammenstoß von Rangierfahrten
		Person wird von Schrankenbaum getroffen
C	Mehrere Leichtverletzte	Aufprall eines Reisezuges auf Gleisabschluss bei niedriger Geschwindigkeit
		Aufprall eines Reisezuges auf Gegenstand bei mittlerer Geschwindigkeit
		Zusammenprall mit nicht führendem Eisenbahnfahrzeug bei niedriger Geschwindigkeit
		Entgleisung eines Reisezuges bei niedriger Geschwindigkeit
		Entgleisung eines Güterzuges bei niedriger Geschwindigkeit
		Zusammenstoß zwischen Güterzügen bei niedriger Geschwindigkeit
D	Ein Schwerverletzter oder viele Leichtverletzte	Aufprall eines Reisezuges auf Gegenstand bei hoher Geschwindigkeit
		Zusammenprall mit führendem Eisenbahnfahrzeug bei niedriger Geschwindigkeit
		Entgleisung eines Güterzuges bei mittlerer Geschwindigkeit
		Zusammenstoß mit einem Reisezug bei niedriger Geschwindigkeit
		Zusammenstoß zwischen Güterzügen bei mittlerer Geschwindigkeit
E	Mehrere Schwerverletzte	Zusammenprall mit nicht führendem Eisenbahnfahrzeug bei mittlerer oder hoher Geschwindigkeit
		Entgleisung eines Reisezuges bei mittlerer Geschwindigkeit
		Entgleisung eines Güterzuges bei hoher Geschwindigkeit
		Zusammenstoß zwischen Güterzügen bei hoher Geschwindigkeit
F	Ein Todesfall oder viele Schwerverletzte	Aufprall eines Reisezuges auf Gleisabschluss bei mittlerer Geschwindigkeit
		Zusammenprall mit führendem Eisenbahnfahrzeug bei mittlerer oder hoher Geschwindigkeit
		Zusammenstoß mit einem Reisezug bei mittlerer Geschwindigkeit
		Personenunfall an höhengleichem Bahnsteigzugang
		Personenunfall in einer Arbeitsstelle
G	Mehrere Todesfälle	Aufprall eines Reisezuges auf Gleisabschluss bei hoher Geschwindigkeit
		Entgleisung eines Reisezuges bei hoher Geschwindigkeit
		Zusammenstoß mit einem Reisezug bei hoher Geschwindigkeit

Anhang C: Zuordnung von Unfallvariablen zu der Opferzahl

Unfallart	Unfallkombination	Geschwindigkeitsklasse	Unfall-geschwindigkeit	Unfallklasse	Anzahl Opfer
Aufprall	GZ	1	$V \approx 0$	A	0
Aufprall	GZ	2	$V \leq 40$	B	0,01
Aufprall	GZ	3	$40 < V \leq 80$	B	0,01
Aufprall	GZ	4	$80 < V \leq 120$	B	0,01
Aufprall	GZ	5	$120 < V \leq 160$	C	0,03
Aufprall	GZ	6	$V > 160$	-	-
Aufprall	RZ	1	$V \approx 0$	A	0
Aufprall	RZ	2	$V \leq 40$	C	0,03
Aufprall	RZ	3	$40 < V \leq 80$	F	1
Aufprall	RZ	4	$80 < V \leq 120$	G	3
Aufprall	RZ	5	$120 < V \leq 160$	H	10
Aufprall	RZ	6	$V > 160$	I	30

Unfallart	Unfallkombination	Geschwindigkeitsklasse	Unfall-geschwindigkeit	Unfallklasse	Anzahl Opfer
Zusammenprall	GZ	1	$V \approx 0$	A	0
Zusammenprall	GZ	2	$V \leq 40$	D	0,1
Zusammenprall	GZ	3	$40 < V \leq 80$	F	1
Zusammenprall	GZ	4	$80 < V \leq 120$	F	1
Zusammenprall	GZ	5	$120 < V \leq 160$	F	1
Zusammenprall	GZ	6	$V > 160$	-	-
Zusammenprall	RZ	1	$V \approx 0$	A	0
Zusammenprall	RZ	2	$V \leq 40$	D	0,1
Zusammenprall	RZ	3	$40 < V \leq 80$	F	1
Zusammenprall	RZ	4	$80 < V \leq 120$	F	1
Zusammenprall	RZ	5	$120 < V \leq 160$	G	3
Zusammenprall	RZ	6	$V > 160$	-	-

Unfallart	Unfallkombination	Geschwindigkeitsklasse	Unfall-geschwindigkeit	Unfallklasse	Anzahl Opfer
Entgleisung	GZ	1	$V \approx 0$	A	0
Entgleisung	GZ	2	$V \leq 40$	C	0,03
Entgleisung	GZ	3	$40 < V \leq 80$	D	0,1
Entgleisung	GZ	4	$80 < V \leq 120$	E	0,3
Entgleisung	GZ	5	$120 < V \leq 160$	F	1
Entgleisung	GZ	6	$V > 160$	-	-
Entgleisung	RZ	1	$V \approx 0$	A	0
Entgleisung	RZ	2	$V \leq 40$	C	0,03
Entgleisung	RZ	3	$40 < V \leq 80$	E	0,3
Entgleisung	RZ	4	$80 < V \leq 120$	G	3
Entgleisung	RZ	5	$120 < V \leq 160$	H	10
Entgleisung	RZ	6	$V > 160$	J	30

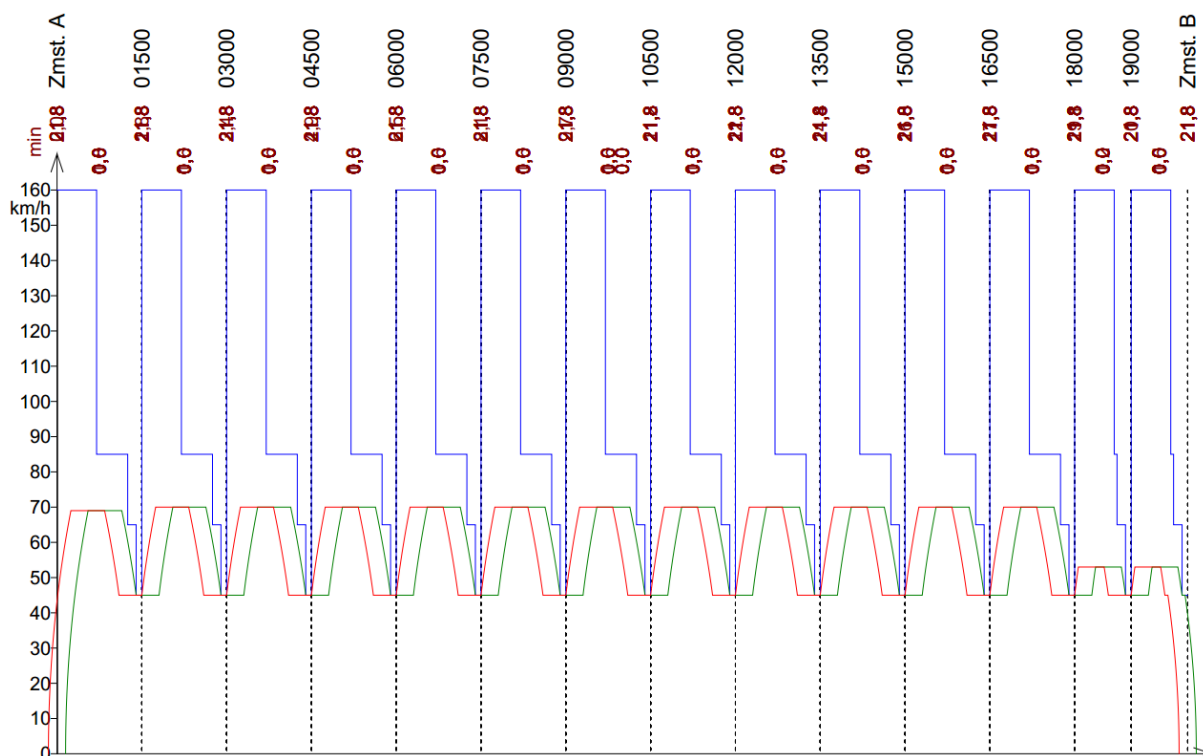
Unfallart	Unfallkombination	Geschwindigkeitsklasse	Unfallgeschwindigkeit	Unfallklasse	Anzahl Opfer
Zusammenstoß	GZ↔GZ	1	$V \approx 0$	A	0
Zusammenstoß	GZ↔GZ	2	$V \leq 40$	C	0,03
Zusammenstoß	GZ↔GZ	3	$40 < V \leq 80$	D	0,1
Zusammenstoß	GZ↔GZ	4	$80 < V \leq 120$	E	0,3
Zusammenstoß	GZ↔GZ	5	$120 < V \leq 160$	F	1
Zusammenstoß	GZ↔GZ	6	$V > 160$	-	-
Zusammenstoß	GZ↔RZ / RZ↔RZ	1	$V \approx 0$	A	0
Zusammenstoß	GZ↔RZ / RZ↔RZ	2	$V \leq 40$	D	0,1
Zusammenstoß	GZ↔RZ / RZ↔RZ	3	$40 < V \leq 80$	F	1
Zusammenstoß	GZ↔RZ / RZ↔RZ	4	$80 < V \leq 120$	G	3
Zusammenstoß	GZ↔RZ / RZ↔RZ	5	$120 < V \leq 160$	H	10
Zusammenstoß	GZ↔RZ / RZ↔RZ	6	$V > 160$	I	30

Unfallart	Unfallkombination	Geschwindigkeitsklasse	Addierte Unfallgeschwindigkeit	Unfallklasse	Anzahl Opfer
Frontalzusammenstoß	GZ↔GZ	1	$V \approx 0$	A	0
Frontalzusammenstoß	GZ↔GZ	2	$V \leq 40$	C	0,03
Frontalzusammenstoß	GZ↔GZ	3	$40 < V \leq 80$	D	0,1
Frontalzusammenstoß	GZ↔GZ	4	$80 < V \leq 120$	E	0,3
Frontalzusammenstoß	GZ↔GZ	5	$120 < V \leq 160$	F	1
Frontalzusammenstoß	GZ↔GZ	6	$V > 160$	F	1
Frontalzusammenstoß	GZ↔RZ / RZ↔RZ	1	$V \approx 0$	A	0
Frontalzusammenstoß	GZ↔RZ / RZ↔RZ	2	$V \leq 40$	D	0,1
Frontalzusammenstoß	GZ↔RZ / RZ↔RZ	3	$40 < V \leq 80$	F	1
Frontalzusammenstoß	GZ↔RZ / RZ↔RZ	4	$80 < V \leq 120$	G	3
Frontalzusammenstoß	GZ↔RZ / RZ↔RZ	5	$120 < V \leq 160$	H	10
Frontalzusammenstoß	GZ↔RZ / RZ↔RZ	6	$V > 160$	I	30

Anhang D: Fahrzeitsimulation zwischen Zmst A und Zmst B

- SPFV
 - Mittlere Beförderungsgeschwindigkeit: 48 km/h
 - Fahrzeitzuschlag: 3 Minuten
 - Zugart PZB 90: Obere Zugart
 - Zugbildung: DB.2x401+4xAvmz801+WSmz804+5xBvmz802
 - Zuglänge: 305 m
 - Max. Geschwindigkeit: 280 km/h

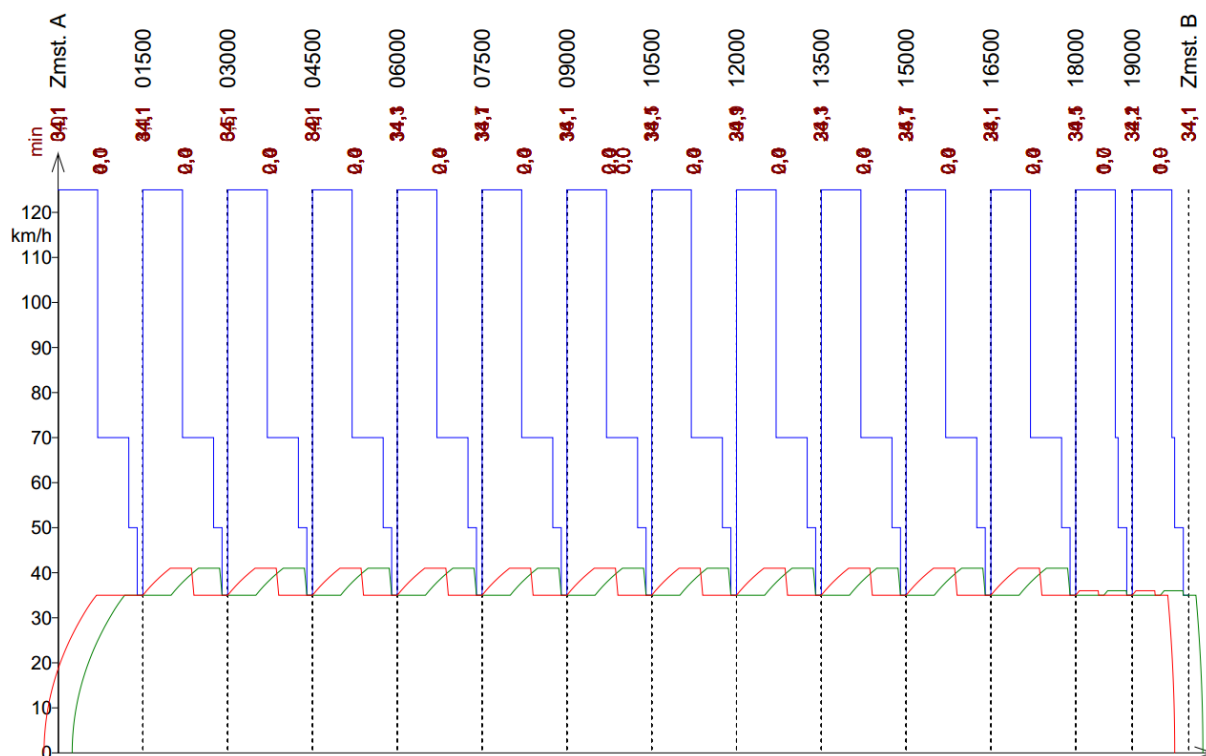
<u>Betriebsstelle</u>	<u>Ankunft</u>	<u>Abfahrt</u>
Zmst. A		6.00
BSig_Ks03000	+0,2	6.04
BSig_Ks04500	+0,2	6.06
BSig_Ks06000	+0,2	6.07
BSig_Ks07500	+0,2	6.09
BSig_Ks09000	+0,2	6.11
BSig_Ks10500	+0,2	6.13
BSig_Ks12000	+0,2	6.15
BSig_Ks13500	+0,2	6.16
BSig_Ks15000	+0,2	6.18
BSig_Ks16500	+0,2	6.20
BSig_Ks18000	+0,2	6.22
Zmst. B	6.25	+0,2



■ **SGV**

- Mittlere Beförderungsgeschwindigkeit: 32 km/h
- Fahrzeitzuschlag: 3 Minuten
- Zugart PZB 90: Mittlere Zugart
- Zugbildung: DB.234+15xTaems893+12xSgss-y703-120
- Zuglänge: 498 m
- Max. Geschwindigkeit: 120 km/h

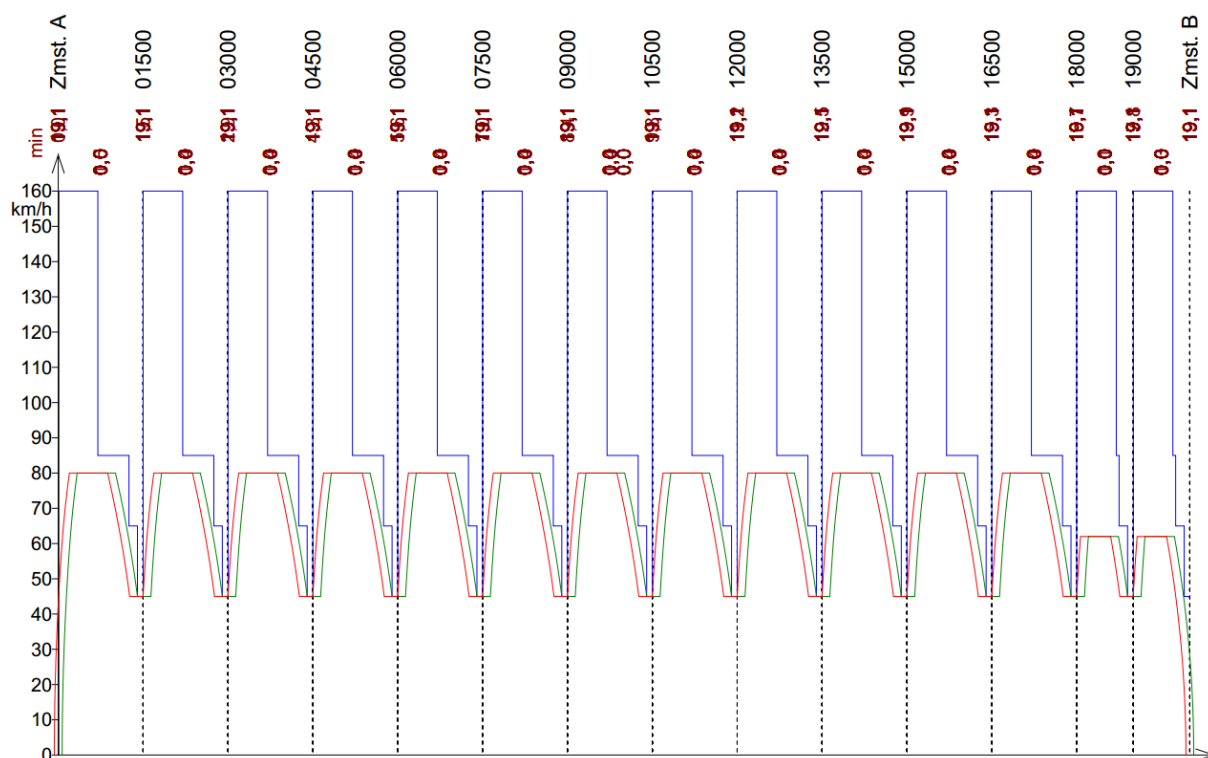
<u>Betriebsstelle</u>	<u>Ankunft</u>	<u>Abfahrt</u>
Zmst. A		6.25
BSig_Ks03000	+0,2	6.32
BSig_Ks04500	+0,2	6.35
BSig_Ks06000	+0,2	6.37
BSig_Ks07500	+0,2	6.40
BSig_Ks09000	+0,2	6.42
BSig_Ks10500	+0,2	6.45
BSig_Ks12000	+0,2	6.48
BSig_Ks13500	+0,2	6.50
BSig_Ks15000	+0,2	6.53
BSig_Ks16500	+0,2	6.56
BSig_Ks18000	+0,2	6.58
Zmst. B	7.02 +0,2	



■ SPNV

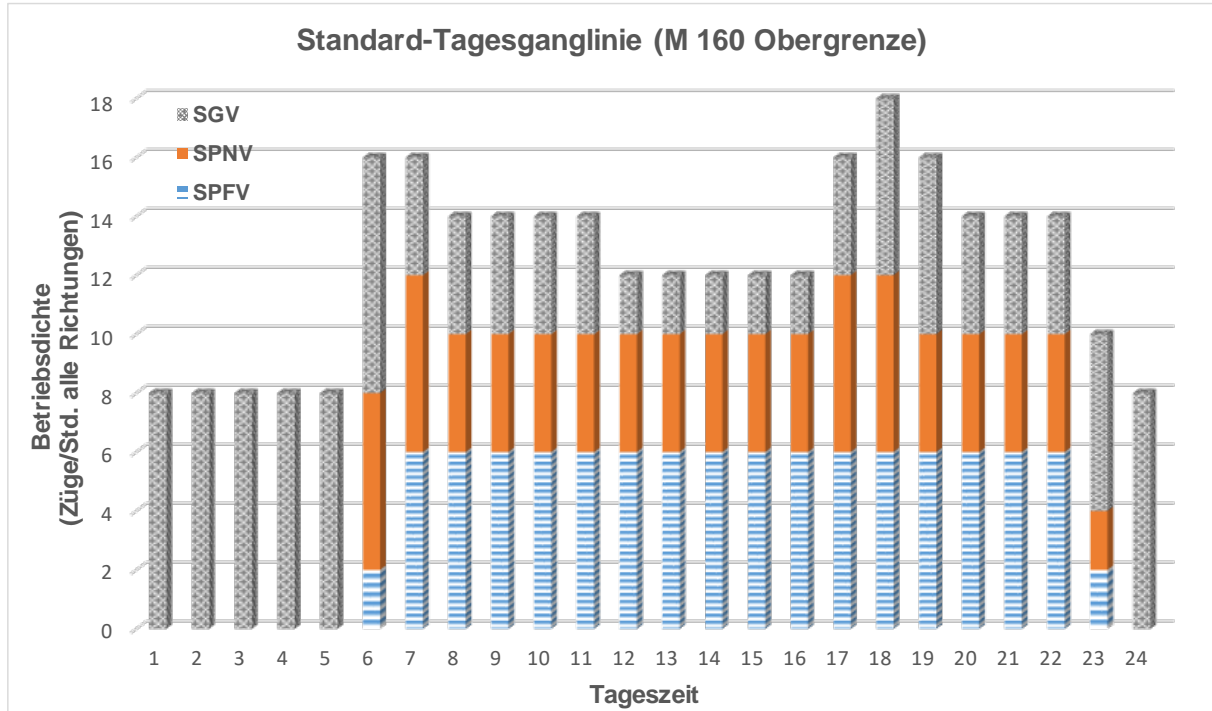
- Mittlere Beförderungsgeschwindigkeit: 54 km/h
- Fahrzeitzuschlag: 3 Minuten
- Zugart PZB 90: Obere Zugart
- Zugbildung: 2xDB.422
- Zuglänge: 138 m
- Max. Geschwindigkeit: 140 km/h

<u>Betriebsstelle</u>	<u>Ankunft</u>	<u>Abfahrt</u>
Zmst. A		7.02
BSig_Ks03000	+0,2	7.05
BSig_Ks04500	+0,2	7.07
BSig_Ks06000	+0,2	7.09
BSig_Ks07500	+0,2	7.10
BSig_Ks09000	+0,2	7.12
BSig_Ks10500	+0,2	7.13
BSig_Ks12000	+0,2	7.15
BSig_Ks13500	+0,2	7.17
BSig_Ks15000	+0,2	7.18
BSig_Ks16500	+0,2	7.20
BSig_Ks18000	+0,2	7.21
Zmst. B	7.24 +0,2	

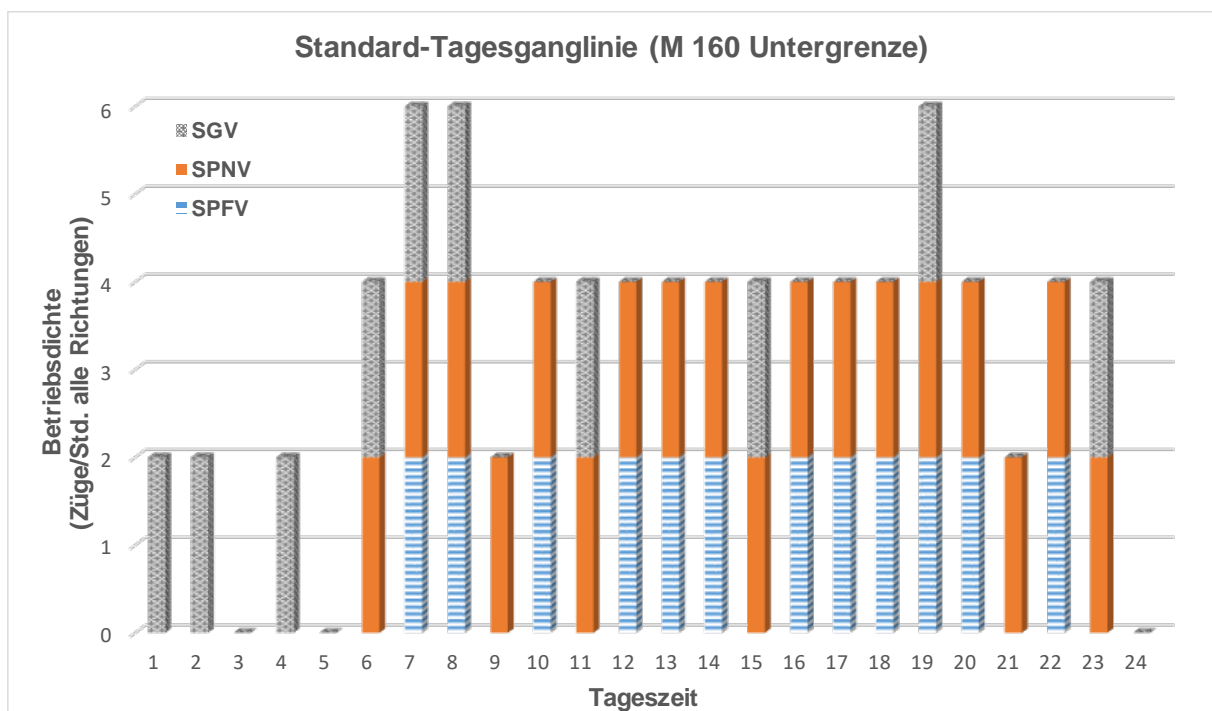


Anhang E: Tagesganglinie Streckenstandard M160

- Standard-Tagesganglinie (M160 Obergrenze) nach [95]
 - 178 Reisezüge und 120 Güterzüge



- Standard-Tagesganglinie (M160 Untergrenze) nach [95]
 - 60 Reisezüge und 20 Güterzüge



Anhang F: Ablaufplan des Rückfallebenenkonzepts A

- Qualitätsindex des Konzepts A:
 - Risikoindex bei 72 Std. Betrieb: 1,82%
 - Leistungsindex bei 72 Std. Betrieb: 60%
- Ablaufplan:

Tag	Std.	Tageszeit	Verkehrszeiten	Variante	Fdl Schicht	Arbeitsstd.	RI	LI
1	1	06	Früh-HVZ	Variante-1	A	1	0,0070%	58%
1	2	07	Früh-HVZ	Variante-1	A	2	0,0070%	58%
1	3	08	Früh-HVZ	Variante-1	A	3	0,0117%	58%
1	4	09	NVZ	Variante-1	A	4	0,0117%	58%
1	5	10	NVZ	Variante-1	A	5	0,0117%	58%
1	6	11	NVZ	Variante-1	A	6	0,0117%	58%
1	7	12	NVZ	Variante-1	A	7	0,0117%	58%
1	8	13	NVZ	Variante-1	A	8	0,0200%	58%
1	9	14	NVZ	Variante-1	B	1	0,0070%	58%
1	10	15	NVZ	Variante-1	B	2	0,0070%	58%
1	11	16	NVZ	Variante-1	B	3	0,0117%	58%
1	12	17	Spät-HVZ	Variante-9	B	4	0,0138%	58%
1	13	18	Spät-HVZ	Variante-9	B	5	0,0138%	58%
1	14	19	Spät-HVZ	Variante-9	B	6	0,0138%	58%
1	15	20	SVZ	Variante-9	B	7	0,0138%	58%
1	16	21	SVZ	Variante-9	B	8	0,0221%	58%
1	17	22	SVZ	Variante-9	C	1	0,0091%	58%
1	18	23	SVZ	Variante-9	C	2	0,0091%	58%
1	19	24	NV	Variante-10	C	3	0,0587%	68%
1	20	01	NV	Variante-10	C	4	0,0587%	68%
1	21	02	NV	Variante-10	C	5	0,0587%	68%
1	22	03	NV	Variante-10	C	6	0,0587%	68%
1	23	04	NV	Variante-10	C	7	0,0587%	68%
1	24	05	NV	Variante-10	C	8	0,0981%	68%
2	1	06	Früh-HVZ	Variante-1	D	1	0,0070%	58%
2	2	07	Früh-HVZ	Variante-1	D	2	0,0070%	58%
2	3	08	Früh-HVZ	Variante-1	D	3	0,0117%	58%
2	4	09	NVZ	Variante-1	D	4	0,0117%	58%
2	5	10	NVZ	Variante-1	D	5	0,0117%	58%
2	6	11	NVZ	Variante-1	D	6	0,0117%	58%
2	7	12	NVZ	Variante-1	D	7	0,0117%	58%
2	8	13	NVZ	Variante-1	D	8	0,0200%	58%
2	9	14	NVZ	Variante-1	E	1	0,0070%	58%
2	10	15	NVZ	Variante-1	E	2	0,0070%	58%
2	11	16	NVZ	Variante-1	E	3	0,0117%	58%
2	12	17	Spät-HVZ	Variante-9	E	4	0,0138%	58%
2	13	18	Spät-HVZ	Variante-9	E	5	0,0138%	58%
2	14	19	Spät-HVZ	Variante-9	E	6	0,0138%	58%
2	15	20	SVZ	Variante-9	E	7	0,0138%	58%
2	16	21	SVZ	Variante-9	E	8	0,0221%	58%

Tag	Std.	Tageszeit	Verkehrszeiten	Variante	Fdl Schicht	Arbeitsstd.	RI	LI
2	17	22	SVZ	Variante-9	F	1	0,0091%	58%
2	18	23	SVZ	Variante-9	F	2	0,0091%	58%
2	19	24	NV	Variante-10	F	3	0,0587%	68%
2	20	01	NV	Variante-10	F	4	0,0587%	68%
2	21	02	NV	Variante-10	F	5	0,0587%	68%
2	22	03	NV	Variante-10	F	6	0,0587%	68%
2	23	04	NV	Variante-10	F	7	0,0587%	68%
2	24	05	NV	Variante-10	F	8	0,0981%	68%
3	1	06	Früh-HVZ	Variante-1	G	1	0,0070%	58%
3	2	07	Früh-HVZ	Variante-1	G	2	0,0070%	58%
3	3	08	Früh-HVZ	Variante-1	G	3	0,0117%	58%
3	4	09	NVZ	Variante-1	G	4	0,0117%	58%
3	5	10	NVZ	Variante-1	G	5	0,0117%	58%
3	6	11	NVZ	Variante-1	G	6	0,0117%	58%
3	7	12	NVZ	Variante-1	G	7	0,0117%	58%
3	8	13	NVZ	Variante-1	G	8	0,0200%	58%
3	9	14	NVZ	Variante-1	H	1	0,0070%	58%
3	10	15	NVZ	Variante-1	H	2	0,0070%	58%
3	11	16	NVZ	Variante-1	H	3	0,0117%	58%
3	12	17	Spät-HVZ	Variante-9	H	4	0,0138%	58%
3	13	18	Spät-HVZ	Variante-9	H	5	0,0138%	58%
3	14	19	Spät-HVZ	Variante-9	H	6	0,0138%	58%
3	15	20	SVZ	Variante-9	H	7	0,0138%	58%
3	16	21	SVZ	Variante-9	H	8	0,0221%	58%
3	17	22	SVZ	Variante-9	I	1	0,0091%	58%
3	18	23	SVZ	Variante-9	I	2	0,0091%	58%
3	19	24	NV	Variante-10	I	3	0,0587%	68%
3	20	01	NV	Variante-10	I	4	0,0587%	68%
3	21	02	NV	Variante-10	I	5	0,0587%	68%
3	22	03	NV	Variante-10	I	6	0,0587%	68%
3	23	04	NV	Variante-10	I	7	0,0587%	68%
3	24	05	NV	Variante-10	I	8	0,0981%	68%

Anhang G: Ablaufplan des Rückfallebenenkonzepts B

- Qualitätsindex des Konzepts B:
 - Risikoindex bei 72 Std. Betrieb: 9,83%
 - Leistungsindex bei 72 Std. Betrieb: 63%
- Ablaufplan:

Tag	Std.	Tageszeit	Verkehrszeiten	Variante	Fdl Schicht	Arbeitsstd.	RI	LI
1	1	06	Früh-HVZ	Variante-5	A	1	0,3647%	68%
1	2	07	Früh-HVZ	Variante-5	A	2	0,3647%	68%
1	3	08	Früh-HVZ	Variante-5	A	3	0,5861%	68%
1	4	09	NVZ	Variante-1	B	1	0,0070%	58%
1	5	10	NVZ	Variante-1	B	2	0,0070%	58%
1	6	11	NVZ	Variante-1	B	3	0,0117%	58%
1	7	12	NVZ	Variante-1	B	4	0,0117%	58%
1	8	13	NVZ	Variante-1	B	5	0,0117%	58%
1	9	14	NVZ	Variante-1	B	6	0,0117%	58%
1	10	15	NVZ	Variante-1	B	7	0,0117%	58%
1	11	16	NVZ	Variante-1	B	8	0,0200%	58%
1	12	17	Spät-HVZ	Variante-5	C	1	0,3647%	68%
1	13	18	Spät-HVZ	Variante-5	C	2	0,3647%	68%
1	14	19	Spät-HVZ	Variante-5	C	3	0,5861%	68%
1	15	20	SVZ	Variante-1	C	4	0,0117%	58%
1	16	21	SVZ	Variante-1	D	1	0,0070%	58%
1	17	22	SVZ	Variante-1	D	2	0,0070%	58%
1	18	23	SVZ	Variante-1	D	3	0,0117%	58%
1	19	24	NV	Variante-10	D	4	0,0587%	68%
1	20	01	NV	Variante-10	D	5	0,0587%	68%
1	21	02	NV	Variante-10	D	6	0,0587%	68%
1	22	03	NV	Variante-10	D	7	0,0587%	68%
1	23	04	NV	Variante-10	D	8	0,0981%	68%
1	24	05	NV	Variante-10	E	1	0,0366%	68%
2	1	06	Früh-HVZ	Variante-5	E	2	0,3647%	68%
2	2	07	Früh-HVZ	Variante-5	E	3	0,5861%	68%
2	3	08	Früh-HVZ	Variante-5	E	4	0,5861%	68%
2	4	09	NVZ	Variante-1	F	1	0,0070%	58%
2	5	10	NVZ	Variante-1	F	2	0,0070%	58%
2	6	11	NVZ	Variante-1	F	3	0,0117%	58%
2	7	12	NVZ	Variante-1	F	4	0,0117%	58%
2	8	13	NVZ	Variante-1	F	5	0,0117%	58%
2	9	14	NVZ	Variante-1	F	6	0,0117%	58%
2	10	15	NVZ	Variante-1	F	7	0,0117%	58%
2	11	16	NVZ	Variante-1	F	8	0,0200%	58%
2	12	17	Spät-HVZ	Variante-5	G	1	0,3647%	68%
2	13	18	Spät-HVZ	Variante-5	G	2	0,3647%	68%
2	14	19	Spät-HVZ	Variante-5	G	3	0,5861%	68%
2	15	20	SVZ	Variante-1	G	4	0,0117%	58%
2	16	21	SVZ	Variante-1	H	1	0,0070%	58%

Tag	Std.	Tageszeit	Verkehrszeiten	Variante	Fdl Schicht	Arbeitsstd.	RI	LI
2	17	22	SVZ	Variante-1	H	2	0,0070%	58%
2	18	23	SVZ	Variante-1	H	3	0,0117%	58%
2	19	24	NV	Variante-10	H	4	0,0587%	68%
2	20	01	NV	Variante-10	H	5	0,0587%	68%
2	21	02	NV	Variante-10	H	6	0,0587%	68%
2	22	03	NV	Variante-10	H	7	0,0587%	68%
2	23	04	NV	Variante-10	H	8	0,0981%	68%
2	24	05	NV	Variante-10	I	1	0,0366%	68%
3	1	06	Früh-HVZ	Variante-5	I	2	0,3647%	68%
3	2	07	Früh-HVZ	Variante-5	I	3	0,5861%	68%
3	3	08	Früh-HVZ	Variante-5	I	4	0,5861%	68%
3	4	09	NVZ	Variante-1	J	1	0,0070%	58%
3	5	10	NVZ	Variante-1	J	2	0,0070%	58%
3	6	11	NVZ	Variante-1	J	3	0,0117%	58%
3	7	12	NVZ	Variante-1	J	4	0,0117%	58%
3	8	13	NVZ	Variante-1	J	5	0,0117%	58%
3	9	14	NVZ	Variante-1	J	6	0,0117%	58%
3	10	15	NVZ	Variante-1	J	7	0,0117%	58%
3	11	16	NVZ	Variante-1	J	8	0,0200%	58%
3	12	17	Spät-HVZ	Variante-5	K	1	0,3647%	68%
3	13	18	Spät-HVZ	Variante-5	K	2	0,3647%	68%
3	14	19	Spät-HVZ	Variante-5	K	3	0,5861%	68%
3	15	20	SVZ	Variante-1	K	4	0,0117%	58%
3	16	21	SVZ	Variante-1	L	1	0,0070%	58%
3	17	22	SVZ	Variante-1	L	2	0,0070%	58%
3	18	23	SVZ	Variante-1	L	3	0,0117%	58%
3	19	24	NV	Variante-10	L	4	0,0587%	68%
3	20	01	NV	Variante-10	L	5	0,0587%	68%
3	21	02	NV	Variante-10	L	6	0,0587%	68%
3	22	03	NV	Variante-10	L	7	0,0587%	68%
3	23	04	NV	Variante-10	L	8	0,0981%	68%
3	24	05	NV	Variante-10	M	1	0,0366%	68%

Anhang H: Ablaufplan des Rückfallebenenkonzepts C

- Qualitätsindex des Konzepts C:
 - Risikoindex bei 72 Std. Betrieb: 19,70%
 - Leistungsindex bei 72 Std. Betrieb: 68%
- Ablaufplan:

Tag	Std.	Tageszeit	Verkehrszeiten	Variante	Fdl Schicht	Arbeitsstd.	RI	LI
1	1	06	Früh-HVZ	Variante-5	A	1	0,3647%	68%
1	2	07	Früh-HVZ	Variante-5	A	2	0,3647%	68%
1	3	08	Früh-HVZ	Variante-5	A	3	0,5861%	68%
1	4	09	NVZ	Variante-8	B1 B2	1	0,2401%	68%
1	5	10	NVZ	Variante-8	B1 B2	2	0,2401%	68%
1	6	11	NVZ	Variante-8	B1 B2	3	0,3647%	68%
1	7	12	NVZ	Variante-8	B1 B2	4	0,3647%	68%
1	8	13	NVZ	Variante-8	C1 C2	1	0,2401%	68%
1	9	14	NVZ	Variante-8	C1 C2	2	0,2401%	68%
1	10	15	NVZ	Variante-8	C1 C2	3	0,3647%	68%
1	11	16	NVZ	Variante-8	C1 C2	4	0,3647%	68%
1	12	17	Spät-HVZ	Variante-5	D	1	0,3647%	68%
1	13	18	Spät-HVZ	Variante-5	D	2	0,3647%	68%
1	14	19	Spät-HVZ	Variante-5	D	3	0,5861%	68%
1	15	20	SVZ	Variante-8	E1 E2	1	0,2401%	68%
1	16	21	SVZ	Variante-8	E1 E2	2	0,2401%	68%
1	17	22	SVZ	Variante-8	E1 E2	3	0,3647%	68%
1	18	23	SVZ	Variante-8	E1 E2	4	0,3647%	68%
1	19	24	NV	Variante-10	F	1	0,0366%	68%
1	20	01	NV	Variante-10	F	2	0,0366%	68%
1	21	02	NV	Variante-10	F	3	0,0587%	68%
1	22	03	NV	Variante-10	F	4	0,0587%	68%
1	23	04	NV	Variante-10	F	5	0,0587%	68%
1	24	05	NV	Variante-10	F	6	0,0587%	68%
2	1	06	Früh-HVZ	Variante-5	G	1	0,3647%	68%
2	2	07	Früh-HVZ	Variante-5	G	2	0,3647%	68%
2	3	08	Früh-HVZ	Variante-5	G	3	0,5861%	68%
2	4	09	NVZ	Variante-8	H1 H2	1	0,2401%	68%
2	5	10	NVZ	Variante-8	H1 H2	2	0,2401%	68%
2	6	11	NVZ	Variante-8	H1 H2	3	0,3647%	68%
2	7	12	NVZ	Variante-8	H1 H2	4	0,3647%	68%
2	8	13	NVZ	Variante-8	I1 I2	1	0,2401%	68%
2	9	14	NVZ	Variante-8	I1 I2	2	0,2401%	68%
2	10	15	NVZ	Variante-8	I1 I2	3	0,3647%	68%
2	11	16	NVZ	Variante-8	I1 I2	4	0,3647%	68%
2	12	17	Spät-HVZ	Variante-5	J	1	0,3647%	68%
2	13	18	Spät-HVZ	Variante-5	J	2	0,3647%	68%
2	14	19	Spät-HVZ	Variante-5	J	3	0,5861%	68%
2	15	20	SVZ	Variante-8	K1 K2	1	0,2401%	68%
2	16	21	SVZ	Variante-8	K1 K2	2	0,2401%	68%

Tag	Std.	Tageszeit	Verkehrszeiten	Variante	Fdl Schicht	Arbeitsstd.	RI	LI
2	17	22	SVZ	Variante-8	K1 K2	3	0,3647%	68%
2	18	23	SVZ	Variante-8	K1 K2	4	0,3647%	68%
2	19	24	NV	Variante-10	L	1	0,0366%	68%
2	20	01	NV	Variante-10	L	2	0,0366%	68%
2	21	02	NV	Variante-10	L	3	0,0587%	68%
2	22	03	NV	Variante-10	L	4	0,0587%	68%
2	23	04	NV	Variante-10	L	5	0,0587%	68%
2	24	05	NV	Variante-10	L	6	0,0587%	68%
3	1	06	Früh-HVZ	Variante-5	M	1	0,3647%	68%
3	2	07	Früh-HVZ	Variante-5	M	2	0,3647%	68%
3	3	08	Früh-HVZ	Variante-5	M	3	0,5861%	68%
3	4	09	NVZ	Variante-8	N1 N2	1	0,2401%	68%
3	5	10	NVZ	Variante-8	N1 N2	2	0,2401%	68%
3	6	11	NVZ	Variante-8	N1 N2	3	0,3647%	68%
3	7	12	NVZ	Variante-8	N1 N2	4	0,3647%	68%
3	8	13	NVZ	Variante-8	O1 O2	1	0,2401%	68%
3	9	14	NVZ	Variante-8	O1 O2	2	0,2401%	68%
3	10	15	NVZ	Variante-8	O1 O2	3	0,3647%	68%
3	11	16	NVZ	Variante-8	O1 O2	4	0,3647%	68%
3	12	17	Spät-HVZ	Variante-5	P	1	0,3647%	68%
3	13	18	Spät-HVZ	Variante-5	P	2	0,3647%	68%
3	14	19	Spät-HVZ	Variante-5	P	3	0,5861%	68%
3	15	20	SVZ	Variante-8	Q1 Q2	1	0,2401%	68%
3	16	21	SVZ	Variante-8	Q1 Q2	2	0,2401%	68%
3	17	22	SVZ	Variante-8	Q1 Q2	3	0,3647%	68%
3	18	23	SVZ	Variante-8	Q1 Q2	4	0,3647%	68%
3	19	24	NV	Variante-10	R	1	0,0366%	68%
3	20	01	NV	Variante-10	R	2	0,0366%	68%
3	21	02	NV	Variante-10	R	3	0,0587%	68%
3	22	03	NV	Variante-10	R	4	0,0587%	68%
3	23	04	NV	Variante-10	R	5	0,0587%	68%
3	24	05	NV	Variante-10	R	6	0,0587%	68%

Anhang I: Ablaufplan des Rückfallebenenkonzepts D

- Qualitätsindex des Konzepts D:
 - Risikoindex bei 72 Std. Betrieb: 18,57%
 - Leistungsindex bei 72 Std. Betrieb: 72%
- Ablaufplan:

Tag	Std.	Tageszeit	Verkehrszeiten	Variante	Fdl Schicht	Arbeitsstd.	RI	LI
1	1	06	Früh-HVZ	Variante-7	A1 A2	1	0,3201%	82%
1	2	07	Früh-HVZ	Variante-7	A1 A2	2	0,3201%	82%
1	3	08	Früh-HVZ	Variante-7	A1 A2	3	0,4862%	82%
1	4	09	NVZ	Variante-8	B1 B2	1	0,2401%	68%
1	5	10	NVZ	Variante-8	B1 B2	2	0,2401%	68%
1	6	11	NVZ	Variante-8	B1 B2	3	0,3647%	68%
1	7	12	NVZ	Variante-8	B1 B2	4	0,3647%	68%
1	8	13	NVZ	Variante-8	C1 C2	1	0,2401%	68%
1	9	14	NVZ	Variante-8	C1 C2	2	0,2401%	68%
1	10	15	NVZ	Variante-8	C1 C2	3	0,3647%	68%
1	11	16	NVZ	Variante-8	C1 C2	4	0,3647%	68%
1	12	17	Spät-HVZ	Variante-7	D1 D2	1	0,3201%	82%
1	13	18	Spät-HVZ	Variante-7	D1 D2	2	0,3201%	82%
1	14	19	Spät-HVZ	Variante-7	D1 D2	3	0,4862%	82%
1	15	20	SVZ	Variante-8	E1 E2	1	0,2401%	68%
1	16	21	SVZ	Variante-8	E1 E2	2	0,2401%	68%
1	17	22	SVZ	Variante-8	E1 E2	3	0,3647%	68%
1	18	23	SVZ	Variante-8	E1 E2	4	0,3647%	68%
1	19	24	NV	Variante-10	F	1	0,0366%	68%
1	20	01	NV	Variante-10	F	2	0,0366%	68%
1	21	02	NV	Variante-10	F	3	0,0587%	68%
1	22	03	NV	Variante-10	F	4	0,0587%	68%
1	23	04	NV	Variante-10	F	5	0,0587%	68%
1	24	05	NV	Variante-10	F	6	0,0587%	68%
2	1	06	Früh-HVZ	Variante-7	G1 G2	1	0,3201%	82%
2	2	07	Früh-HVZ	Variante-7	G1 G2	2	0,3201%	82%
2	3	08	Früh-HVZ	Variante-7	G1 G2	3	0,4862%	82%
2	4	09	NVZ	Variante-8	H1 H2	1	0,2401%	68%
2	5	10	NVZ	Variante-8	H1 H2	2	0,2401%	68%
2	6	11	NVZ	Variante-8	H1 H2	3	0,3647%	68%
2	7	12	NVZ	Variante-8	H1 H2	4	0,3647%	68%
2	8	13	NVZ	Variante-8	I1 I2	1	0,2401%	68%
2	9	14	NVZ	Variante-8	I1 I2	2	0,2401%	68%
2	10	15	NVZ	Variante-8	I1 I2	3	0,3647%	68%
2	11	16	NVZ	Variante-8	I1 I2	4	0,3647%	68%
2	12	17	Spät-HVZ	Variante-7	J1 J2	1	0,3201%	82%
2	13	18	Spät-HVZ	Variante-7	J1 J2	2	0,3201%	82%
2	14	19	Spät-HVZ	Variante-7	J1 J2	3	0,4862%	82%
2	15	20	SVZ	Variante-8	K1 K2	1	0,2401%	68%
2	16	21	SVZ	Variante-8	K1 K2	2	0,2401%	68%

Tag	Std.	Tageszeit	Verkehrszeiten	Variante	Fdl Schicht	Arbeitsstd.	RI	LI
2	17	22	SVZ	Variante-8	K1 K2	3	0,3647%	68%
2	18	23	SVZ	Variante-8	K1 K2	4	0,3647%	68%
2	19	24	NV	Variante-10	L	1	0,0366%	68%
2	20	01	NV	Variante-10	L	2	0,0366%	68%
2	21	02	NV	Variante-10	L	3	0,0587%	68%
2	22	03	NV	Variante-10	L	4	0,0587%	68%
2	23	04	NV	Variante-10	L	5	0,0587%	68%
2	24	05	NV	Variante-10	L	6	0,0587%	68%
3	1	06	Früh-HVZ	Variante-7	M1 M2	1	0,3201%	82%
3	2	07	Früh-HVZ	Variante-7	M1 M2	2	0,3201%	82%
3	3	08	Früh-HVZ	Variante-7	M1 M2	3	0,4862%	82%
3	4	09	NVZ	Variante-8	N1 N2	1	0,2401%	68%
3	5	10	NVZ	Variante-8	N1 N2	2	0,2401%	68%
3	6	11	NVZ	Variante-8	N1 N2	3	0,3647%	68%
3	7	12	NVZ	Variante-8	N1 N2	4	0,3647%	68%
3	8	13	NVZ	Variante-8	O1 O2	1	0,2401%	68%
3	9	14	NVZ	Variante-8	O1 O2	2	0,2401%	68%
3	10	15	NVZ	Variante-8	O1 O2	3	0,3647%	68%
3	11	16	NVZ	Variante-8	O1 O2	4	0,3647%	68%
3	12	17	Spät-HVZ	Variante-7	P1 P2	1	0,3201%	82%
3	13	18	Spät-HVZ	Variante-7	P1 P2	2	0,3201%	82%
3	14	19	Spät-HVZ	Variante-7	P1 P2	3	0,4862%	82%
3	15	20	SVZ	Variante-8	Q1 Q2	1	0,2401%	68%
3	16	21	SVZ	Variante-8	Q1 Q2	2	0,2401%	68%
3	17	22	SVZ	Variante-8	Q1 Q2	3	0,3647%	68%
3	18	23	SVZ	Variante-8	Q1 Q2	4	0,3647%	68%
3	19	24	NV	Variante-10	R	1	0,0366%	68%
3	20	01	NV	Variante-10	R	2	0,0366%	68%
3	21	02	NV	Variante-10	R	3	0,0587%	68%
3	22	03	NV	Variante-10	R	4	0,0587%	68%
3	23	04	NV	Variante-10	R	5	0,0587%	68%
3	24	05	NV	Variante-10	R	6	0,0587%	68%